all rights reversed

HACKER

Season 05 / Issue 03

τεύχος 051 - Cease-and-Desist Edition

Ξέγνοιαστο BitTorrenting [*]

Δημιουργία του δικού μας Seedbox

Ανώνυμο VPN με πολλαπλά σημεία εξόδου

Υπηρεσίες Active Directory, χωρίς active-τσέπη

Χρήση iptables για προστασία privacy/anonymity

Πολλαπλές συνδέσεις VPN, από το ίδιο pfSense box

[*] ...με δικλείδες ασφαλείας!

all rights reversed

HACKER



CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Νίκος Μουρατίδης, Βούλα Παυλίδου
Σύνταξη	Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Γιώργος Γιάννου, Μανώλης Κιαγιάς, Πέτρος Κυλαδίτης, Νίκος Μουρατίδης, Θωμάς Σερμπίνης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας, @arkoudos
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ηλεκτρονικό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations δώδεκα φορές το χρόνο, κάθε μήνα. Η Parabing Creations έχει την έδρα της στην Καλαμαριά Θεσσαλονίκης. Ο δικτυακός τόπος του περιοδικού είναι στο http://deltahacker.gr. Το email επικοινωνίας είναι το talk2us@deltahacker.gr και ειδικά για τις συνδρομές είναι το subscriptions@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο http://deltahacker.gr/pdf12order και από την ίδια σελίδα γίνονται οι παραγγελίες συνδρομών.


deltaHacker Field Bag
€25.50
MORE COLORS AVAILABLE
deltaHacker Mugs
€12.50
deltaHacker Thermos® Can Cooler
€17.50
QUESTIONS? | ORDER BY PHONE? | CALL 1-877-809-1659
Where's My Stuff?
Track your recent orders.
View or change your order.
Shipping & Returns
See our shipping rates.
Make a return or exchange.
Need Help?
Satisfaction Guaranteed.
Visit our Customer Service.
CafePress.com. All rights reserved.
is powered by CafePress Inc. Copyright © 1999-2015 CafePress.com. All rights reserved.
olicy | Trademark & Copyright Information
urrency rates are updated daily and may fluctuate.
Δώρα με στιλ, που έχουν *αληθινή* αξία.
Όλα στο μαγαζάκι του deltaHacker,
κάτω από το Cafepress.
Περάστε μια βόλτα από το
http://www.cafepress.co.uk/deltahacker
–σας περιμένουμε!

Παράλληλα σύμπαντα

του Χρήστου Βαρελά

Αγαπητές κι αγαπητοί, φίλες και φίλοι, συντρόφισσες και σύντροφοι.

- Αυτή τη στιγμή, το κουράγιο για την πληκτρολόγηση των γραμμών αυτών είναι κάτι που μου λείπει.
- Δυσκολεύτηκα πολύ για να ξεκινήσω το κείμενο, ενώ ξέρω ότι θα δυσκολευτώ περίπου 129 φορές περισσότερο για να το ολοκληρώσω.
- Είμαι συγκλονισμένος, ανήσυχος και φοβισμένος.
- Σιγά, όλοι είμαστε απ' όλα αυτά, θα σκεφτείτε. Υπάρχει κανείς ατάραχος, ήρεμος κι εντελώς γενναίος, με όλα όσα γίνονται τον τελευταίο καιρό;
- Ναι, έτσι είναι όπως τα λέτε, δεν το συζητώ.
- Αλλά πριν μία περίπου εβδομάδα διάβασα μια είδηση και σκιάχτηκα ακόμα πιο πολύ.
- Είναι ένας κος Καθηγητής από το Πανεπιστήμιο της Uppsala, στη Σουηδία, ο οποίος μετά από (πολλές) πράξεις έφτασε σ' ένα συμπέρασμα που αλλάζει τα πάντα. Αναφέρομαι στον Erik Zackrisson, έγκριτο Αστροφυσικό, ο οποίος βάλθηκε να υπολογίσει την πιθανότητα ύπαρξης πλανήτου παρομοίου με τον δικό μας, ο οποίος θα μπορεί να υποστηρίξει τη ζωή όπως την ξέρουμε – ή μια ζωή που κάπως θα της μοιάζει, τέλος πάντων.
- Λοιπόν, για να βεβαιωθώ ότι θα κατανοήσετε τι μου συνέβη όταν διάβασα για τα αποτελέσματα της έρευνας του κου Καθηγητού, θα κάνω εδώ ένα αναπάντεχο, δραματικό αλλά σύντομο διάλειμμα για τη μετάδοση μιας άλλης είδησης. Έτσι, αν μη τι άλλο για να έχετε και λίγο περισσότερο χρόνο ώστε να προετοιμαστείτε ψυχολογικά για τον κο Zackrisson.
- **Διάλειμμα:** *Επιτυχημένη επίθεση πραγματοποιήθηκε στο site της δημοφιλούς διανομής Linux Mint, με αποτέλεσμα οι επισκέπτες να κατεβάζουν μολυσμένα ISO images της εκδοχής Cinnamon, από κακόβουλους FTP servers. Οι εν λόγω servers βρίσκονταν στη Βουλγαρία και το τροποποιημένο ISO περιελάμβανε το TSUNAMI, ένα απλοϊκό για τα σημερινά δεδομένα IRC bot που χρησιμοποιείται για την πραγματοποίηση επιθέσεων DDoS. Το γεγονός ότι οι επιτιθέμενοι δεν ενσωμάτωσαν πιο ύπουλο ή/και πιο επικερδές malware, όπως, π.χ., θα ήταν ένας Bitcoin miner, οδηγεί τους αναλυτές στο συμπέρασμα ότι μάλλον πρόκειται για νεοφερμένους στο χώρο. Η κατάσταση πλέον έχει τεθεί υπό έλεγχο κι από το site του Linux Mint διανέμονται τα επίσημα ISO images.*
- Επιστρέφουμε τώρα στη μελέτη του κου Καθηγητού.
- Βαθιά ανάσα κι ας ξεκινήσουμε με τη μεγάλη εικόνα.

/var/log/messages

- Στο γαλαξία μας και μόνο υπάρχουν περί τα 50 δισεκατομμύρια πλανήτες. Δεν αναφέρομαι σε συνηθισμένους πλανήτες. Όχι, αυτοί είναι πολλοί περισσότεροι. Αυτά τα 50 δισεκατομμύρια πλανήτες του γαλαξία μας που μόλις ανέφερα, είναι εκείνοι που ομοιάζουν με τη Γη και που θα μπορούσαν να υποστηρίξουν τη ζωή όπως την ξέρουμε. Οι μαθηματικές πιθανότητες, λοιπόν, υπαγορεύουν ότι έστω και σε έναν από αυτούς –της Γης εξαιρουμένης– θα μπορούσε να υπάρχει ζωή όπως τη γνωρίζουμε.
- Η πιθανότητα να μην είμαστε μόνοι γίνεται ακόμα μεγαλύτερη, αν σκεφτούμε ότι εκτός από το γαλαξία μας, στο Σύμπαν υπάρχουν περίπου άλλα 100 δισεκατομμύρια γαλαξίες. Δεν χρειάζεται να παίζεις στα δάκτυλα τη Θεωρία Πιθανοτήτων, για να δεχτείς ότι *αποκλείεται* να είμαστε μόνοι μας. Εντάξει, ίσως είναι ιλιγγιωδώς απίθανο να συναντήσουμε όντα από άλλους πλανήτες, ωστόσο η βεβαιότητα ότι είναι κάπου Εκεί Έξω (TM) είναι αρκετή για να καθησυχάζει τις υπαρξιακές μας ανησυχίες.
- Όλα ωραία, λοιπόν, αλλά όχι για τον κο Καθηγητή. Ο Erik Zackrisson δεν είναι από εκείνους που παίζουν αφελώς με τις πιθανότητες για να φτάνουν σε σαθρά συμπεράσματα. Έφτιαξε λοιπόν ένα μοντέλο σε υπολογιστή και το άφησε να τρέξει. Λαμβάνοντας υπόψη ό,τι γνωρίζουμε για τους εξωπλανήτες κι όλα όσα η Φυσική υποδεικνύει πως συνέβησαν μετά τη Μεγάλη Έκρηξη –μιλάμε τώρα για ένα διάστημα 13,8 δισεκατομμυρίων ετών–, το μοντέλο επιχείρησε να υπολογίσει την πιθανότητα ύπαρξης πλανήτη παρόμοιου με τη Γη *και* με ζωή.
- Και πράγματι, την υπολόγισε την πιθανότητα.
- Από ένα σύνολο 7 x 10^20 πλανητών στο Σύμπαν, ζωή έχει ένας και μόνον ένας: ο δικός μας.
- Η ζωή στον πλανήτη μας όχι μόνο δεν είναι ο κανόνας, αλλά δεν είναι καν η εξαίρεση.
- Όχι. Είναι απλά μια στατιστική ανωμαλία, κάτι το οποίο δεν είχε λόγο να συμβεί κι όμως, εντελώς από λάθος, συνέβη.
- Ο κος καθηγητής έφτασε στο συμπέρασμά του βασιζόμενος σε μοντέλο – και τα μοντέλα εξ ορισμού αποτελούν προσεγγίσεις της πραγματικότητας. Ίσως, λοιπόν, κάτι να του ξεφεύγει και τελικά να μην είμαστε μόνοι μας.
- Εδώ δεν έλαβε καν υπόψη του τα παράλληλα σύμπαντα, θα σκεφτεί κάποιος. Και τη σκέψη αυτού του κάποιου δεν πρέπει να βιαστούμε και να την απορρίψουμε, αγαπητές κι αγαπητοί. Θυμηθείτε: Τέλεια γνώση δεν έχουμε, στα σκοτάδια κινούμαστε και ψηλαφίζουμε.
- Μπορεί, λοιπόν, ο κος καθηγητής να έχει δίκιο και στο δικό μας Σύμπαν να επικρατεί ησυχία, τάξη και ασφάλεια –τουλάχιστον σε μια κοσμική κλίμακα–, αλλά την ίδια στιγμή να υπάρχουν και παράλληλα σύμπαντα. Σε κάποια από αυτά είναι πιθανό να υπάρχει ζωή σε περισσότερους από έναν πλανήτες. Σε κάποιο άλλο, ίσως υπάρχει ζωή σε καμιά πενηνταριά πλανήτες. Σε παράλλο παίζει να επικρατεί ενοχλητικός

συνωστισμός και οι εκεί επιστήμονες να συζητούν για την ύπαρξη ησύχων συμπάντων, σαν το δικό μας. Ποιος ξέρει; Ποιος μπορεί με βεβαιότητα να πει; Ποιος είναι πρόθυμος να αποκλείσει τη μία και την άλλη υπόθεση;

- Τελικά, ξεκίνησα να γράφω το κείμενο αυτό με βαριά καρδιά, όσο όμως το σκέφτομαι αισιοδοξώ. Ναι, αν όχι στο δικό μας τότε σίγουρα σε κάποιο άλλο, παράλληλο Σύμπαν, να υπάρχει ζωή εδώ κι εκεί και παραπέρα.
- Αλλά, για μια στιγμή. Θα μπορέσουμε άραγε κάποια στιγμή να είμαστε σίγουροι; Θα καταφέρουμε, με κάποιο τρόπο, να πεταχτούμε σε ένα ή δύο παράλληλα σύμπαντα; Όχι για να τους κατσικωθούμε, δεν είμαστε τέτοιοι εμείς. Απλά, για να ρίξουμε μια ματιά στους εκεί φυσικούς νόμους και μετά να γυρίσουμε αμέσως στο δικό μας σύμπαν, ώστε να βελτιώσουμε τα μοντέλα μας.
- Θα μου πείτε, εδώ δυσκολευόμαστε να πάμε μέχρι τον Άρη, ενώ και το ταξίδι μέχρι την άκρη του ηλιακού μας συστήματος αποτελεί μέγιστο καζίκι. Μετά βέβαια έχουμε και το γαλαξία μας και ύστερα ένα σωρό άλλους γαλαξίες στο δικό μας μας σύμπαν. Δεν μπορούμε, κατά πώς φαίνεται, να πάμε λίγο πιο πέρα από την αυλή μας – και τα παράλληλα σύμπαντα μάς μάραναν!
- Δίκιο έχετε. Όσο κι αν η συλλογιστική σας φέρνει ξανά το φόβο, δεν μπορώ παρά να παραδεχτώ ότι έχετε δίκιο. Εκτός βέβαια κι αν σκεφτόμαστε λάθος. Ίσως, π.χ., η μετάβαση σε παράλληλο σύμπαν να μην προϋποθέτει ότι πρέπει πρώτα να διασχίσουμε το παρόν σύμπαν. Μπορεί το μόνο που χρειαζόμαστε να είναι το κατάλληλο shortcut στους νόμους της Φυσικής και μετά θα μπορούμε να πεταγόμαστε από σύμπαν σε σύμπαν, να κάνουμε τις παρατηρήσεις μας, να πραγματοποιούμε μερικές αθώες ρυθμίσεις και να επιστρέφουμε εδώ, στα γνωστά τα μέρη.
- Είναι άραγε κάτι τέτοιο εφικτό ή το όλο σκεπτικό συγγενεύει με ευχολόγιο;
- Τι να σας πω, πραγματικά δεν ξέρω. Πάντως η αισιόδοξη πλευρά του χαρακτήρα μου έχει αρχίσει και πάλι να κερδίζει έδαφος. Ναι, νομίζω ότι η μετάβαση σε παράλληλα σύμπαντα *είναι* εφικτή.
- Τώρα που το σκέφτομαι λίγο πιο ψύχραιμα, τολμώ και θεωρώ ότι κάποιοι συμπολίτες μας πρέπει *ήδη* να ζουν σε παράλληλα σύμπαντα. Αν μάλιστα η υπόθεσή μου δεν είναι λανθασμένη, εξηγεί πολλά. Να, θα αναφέρω ένα-δυο παραδείγματα στην τύχη. Ορισμένοι συμπολίτες μας δεν φαίνεται να παραξενεύονται καθόλου όταν το ΟΧΙ μετατρέπεται σε ΝΑΙ. Μην το σκέφτεστε με τη λογική του δικού μας σύμπαντος: Είναι που στο δικό τους σύμπαν οι νόμοι της φύσης επιτρέπουν τέτοιου είδους απότομες μεταβάσεις. Αποτελούν καθημερινό κι εντελώς βαρετό φαινόμενο στον κόσμο τους, πώς να το κάνουμε. Άλλο παράδειγμα: Υπάρχουν συμπολίτες μας που πιστεύουν ότι η κυβέρνηση έχει σχέδιο, ξέρει πολύ καλά τι κάνει και τελικά όλα θα πάνε καλά. Μη γελάτε. Στο δικό τους σύμπαν όλα αυτά συμβαίνουν ήδη. Αν ήμαστε κι εμείς στο ίδιο σύμπαν, παρόμοια θα σκεφτόμασταν, τα ίδια θα λέγαμε.
- Αλλά δεν είμαστε.

POST CAR

THE ADDRESS TO BE WRITTEN ON THIS SID



σνέιλ μέιλ

Αγαπητοί μου,

Κινητικότητα σήμερα στο σπίτι και σας γράφω στα γρήγορα.

Προ ολίγου είχε έρθει ο κύριος Κώστας από την Εβγα για να αφήσει ένα βίντεο.

Βίντεο, ναι. (Γιου νόου, βίντεο; Από εκείνα με τις βιντεοκασέτες;)

Το έφερε σε μια αρχαία σακούλα από το Μινιόν και το άφησε στο τραπέζι. Σε μια άλλη σακούλα έχει φέρει δύο βιντεοκασέτες. Τετράωρες απ' ό,τι μας εξήγησε.

Καταφέρνει και τις βρίσκει, κοψοτιμής λέει, από έναν προμηθευτή του που έχει τα κατάλληλα κονέ και μπορεί να σου βρει οτιδήποτε.

"Πάντως βρίσκεις. Άμα θέλεις, βρίσκεις", μου είπε μειλίχια, βλέποντας το ανήσυχό μου βλέμμα. "Δεν υπάρχει πρόβλημα."

Αυτό που ο κύριος Κώστας ξέχασε να φέρει, είναι το καλώδιο για να συνδέσουμε το βίντεο με την τηλεόραση. Εφυγε για να το φέρει.

Περιμένοντάς τον, όλοι είμαστε απασχολημένοι με κάτι.

Εγώ σας γράφω την επιστολή. Η μητέρα της Εξαδέλφης, που είναι ινδουίστρια, και η Κυρία Καίτη, ετοιμάζουν στην κουζίνα καυτερά σαμοσάκια λαχανικών, κοτομπουκιές με κάρυ, και πανήρ με σπανάκι. Η Εξαδέλφη είναι κάπου εδώ γύρω και δεν συμμετέχει ιδιαίτερα, και η Μαιρούλα προσπαθεί να συνδεθεί με το Σκάιπ αλλά κάτι έχει συμβεί σήμερα και το ίντερνετ σέρνεται.

Τελευταία Κυριακή του Ιανουαρίου, που λέτε, και έχουμε αποφασίσει να τιμήσουμε την επέτειο με βραδιά βίντεο, ινδικό μπουφέ και σάλατ μπαρ.

Η έμπνευση μάς ήρθε από τις αφίσες που έχουν γεμίσει την Αθήνα, για την εκδήλωση στο τάε κβον ντο.

"Ένας Χρόνος Μάχη -- Προχωράμε", και τα λοιπά. Θα τις έχετε δει, δεν μπορεί.

Α, όλα κι όλα, η φτώχια θέλει καλοπέραση.

Η Μαιρούλα, την είχε πιάσει το αγωνιστικό της, έλεγε να πάει. Η Κυρία Καίτη, από την άλλη, ανησυχούσε και δεν ήθελε να την αφήσει. Τελικά ο καυγάς αποφεύχθηκε όταν έπεσε η ιδέα της βιντεοβραδιάς.

Που λέτε, αποδεικνύεται πως ο κύριος Κώστας έχει αρχείο βιντεοκασετών με όλες τις βραδιές αποτελεσμάτων εκλογών από το 2000 και μετά. Το άκουγα που το 'λεγε προ ημερών στην ομήγυρη και δεν το πίστευα. Τις έχει όλες, εθνικές εκλογές από 2000 και μετά, βιντεογραμμένες. Real time.

Ξεκινάει να γράφει από τα πρώτα έξιτ πολ, μετά τα αποτελέσματα έτσι ως έρχονται, τις συζητήσεις, τις συνεντεύξεις και τα λοιπά. Επί όσο πάρει. Συνήθως δύο τετράωρες βιντεοκασέτες. Καμιά φορά και τρεις.

Ετσι έκανε πέρσυ. Η ιστορική νίκη του λαού απέναντι στη νεοφιλελεύθερη λαίλαπα είναι μαγνητοσκοπημένη και έτοιμη για όποιον ενδιαφέρεται να αναθερμάνει τα αγωνιστικά του πιστεύω.

Με το που έπεσε, λοιπόν, η ιδέα, στείλαμε στην Εβγα την Κυρία Καίτη με τη Μαιρούλα να κανονίσουν τις λεπτομέρειες, και η συμφωνία έκλεισε.

Ο Κύριος Κώστας θα βάλει βίντεο και βιντεοκασέτες (το καλώδιο ξέχασε, αλλά το φέρνει τώρα) κι εμείς θα βάλουμε Ινδικό μπουφέ και σπίτι. Λευκές μπύρες ρυζιού Χαντία αγοράσαμε από το ινδονησιακό σουπερμάρκετ στη γωνία, που τις φέρνει απευθείας από το Μάντγια Πραντές. Από εκεί αγοράσαμε και κρακεράκια ρυζιού (για τις πίκλες τσίλι) και μείγμα Τσάνα Χουρ για σνακ.

Γενικώς είμαστε πανέτοιμοι να χαιρετίσουμε εορταστικά την εορταστική αυτή εορτή.

Ειδικά το Τσάνα Χουρ θα το σερβίρουμε με ψιλοκομμένο κρεμμύδι μαϊντανό και μπόλικο γιαούρτι, γιατί καίει σαν την κόλαση. Ελπίζω να βοηθήσει και η μπύρα ρυζιού.

Τέλος πάντων, το σκεφτήκαμε ψύχραιμα: Αν είναι να ανάψεις από κάτι καλύτερα να ανάψεις από το Τσάνα Χουρ, παρά από την συζήτηση.

Θα ήθελα πάντως --αν με ρωτήσετε θα το παραδεχτώ-- θα ήθελα να μπορούσαμε να κάνουμε μια σοβαρή, και ψύχραιμη κατά το δυνατόν, συζήτηση για όσα συνέβησαν στην Ελλάδα τους τελευταίους 12 μήνες.

Θα το ήθελα --αλλά μοιάζω να είμαι ο μόνος που το θέλει. Όλοι είναι πλέον περιχαρακωμένοι πίσω από εκατέρωθεν γραμμές Μαζινό και δεν σηκώνουν μύγα στο σπαθί τους.

Θα θυμάστε, σας τα έλεγα και την περασμένη φορά. Ο δημόσιος διάλογος στη χώρα μας leaves much to be desired που λένε και οι κουτόφραγκοι.

Εχουμε μάλιστα φτάσει σε ένα σημείο που και μόνο το να θέσεις θέμα διαλόγου και ανταλλαγής απόψεων σε κατατάσσει αυτομάτως στο στρατόπεδο των φιλελέδων, των ευροφλώρων, και του ακραίου κέντρου. Κι αν όχι αυτομάτως, σίγουρα πάντως νομοτελειακά.

Διότι, βέβαια, τι άλλο θα ήσουν αν όχι φιλελεύθερο θατσερικό γουρούνι, ή αφελής ηλίθιος, αν αρνείσαι να δεις ότι το μεγάλο κεφάλαιο και το 1% έχουν εξαπολύσει κατά μέτωπον επίθεση σε κάθε κατάκτηση του εργατικού κινήματος, με στόχο να καταργήσουν κάθε έννοια κοινωνικού κράτους.

Αν μάλιστα ζητήσεις διευκρινίσεις και κάνεις το λάθος να επισημάνεις πως --ανεξαρτήτως του ενδεχόμενου να υφίσταται όντως επίθεση το κοινωνικό κράτος εκ μέρους του μεγάλου κεφαλαίου και του 1%-- το πρόβλημα της Ελλάδας είναι διαφορετικό, πως στην Ελλάδα ούτως ή άλλως δεν υπήρχε κοινωνικό κράτος (τουλάχιστον με την έννοια που υπάρχει στην Ευρώπη), και ότι, strictly speaking, δεν τίθεται θέμα κατάργησής του, θα σε κοιτάξουν με απέχθεια και οίκτο.



Αν τελικά κάνουν τον κόπο να σου απαντήσουν, θα σου πούνε ότι κάθε χώρα είναι διαφορετική, και πως, εν πάση περιπτώσει, αυτό που είχαμε στην Ελλάδα, *αυτό* έχουν βάλει στο στόχαστρο, το μεγάλο νεοφιλελεύθερο πείραμα γίνεται στα κεφάλια μας, τυφλός είσαι και δεν το βλέπεις;

Θα απαντήσεις βέβαια πως δυσκολεύεσαι να το δεις, γιατί ξέρεις πως άλλο πράγμα το κόστος του κοινωνικού κράτους, και άλλο πράγμα το κόστος του κράτους γενικά. Θα τους πεις πως αν ακόμα και σήμερα το κόστος της κακοδιαχείρισης και της διαφθοράς στο Ελληνικό κράτος ανέρχεται στα 33 δισεκατομμύρια ετησίως (γκουκλ!), τότε, κατά τη γνώμη σου, καλώς κάνουν οι ευρωπαίοι και αρνούνται να συνεχίσουν να το χρηματοδοτούν, και μας ζητούν να λάβουμε τα μέτρα μας. Κι ότι στο χέρι μας είναι να αποφασίσουμε τι να κάνουμε.

Θα σε κοιτάξουν με συγκρατημένη οργή ανάκατη με αηδία και θα σου πούνε για τις αυτοκτονίες και τα παιδιά που πεινάνε στα σχολεία.

Ή μάλλον όχι. Δεν θα σου πούνε για τις αυτοκτονίες και τα παιδιά που πεινάνε στα σχολεία, γιατί πλέον πνέει άλλος αέρας στη χώρα τους τελευταίους 12 μήνες και οι αυτοκτονίες έχουν κοπεί με το μαχαίρι. Χώρια που τα παιδιά δεν πεινάνε πλέον.

Οπότε δεν θα σου απαντήσουν καν.

Γιατί; Δεν ξέρω. Υποθέτω πως θεωρούν ότι δεν έχει νόημα να απαντάει κανείς σε κάποιον που από άγνοια, αφέλεια ή συμφέρον αρνείται να δει πως το πρόβλημα του καπιταλισμού είναι δομικό και πως η κρατική διαφθορά είναι ένα πρόσκαιρο σύμπτωμα, ένα επιφαινόμενο. Υποθέτω πως πιστεύουν πως όταν εμμένει κανείς στη διαφθορά, στην κακοδιαχείριση και στη φοροδιαφυγή, συμβάλλει όχι στη λύση του προβλήματος της Ελλάδας, αλλά στη διαιώνισή του.

Υποθέτω πως θα έχουν στο μυαλό τους κάποια "μεγάλη εικόνα", που τους βοηθάει να ερμηνεύσουν την εμμονή στα 33 δις της διαφθοράς του δημόσιου τομέα, ως αυτό που πραγματικά είναι: Μια ψευδο-μεταρρυθμιστική φενάκη, μια νεοφιλελεύθερη παγίδα, ένα θατσερικό άλλοθι, μια κερκόπορτα που θα οδηγήσει στην ήττα του εργατικού κινήματος, στην εξαθλίωση της αγροτιάς και στο ξεπούλημα της κρατικής περιουσίας (όχι απαραίτητα με αυτή την σειρά).

Υποθέτω πως είναι η ίδια "μεγάλη εικόνα" που τους επιτρέπει να αγνοούν τις ηρωικές τελετές για τα 3210 χρόνια από τον Τρωικό Πόλεμο, ή τους κάθε λογής ξαδέλφους και κουμπάρους που τοποθετούνται ως μετακλητοί εδώ κι εκεί.

Μπροστά στη μεγάλη εικόνα όλα όσα θα μπορούσα να πω είναι λεπτομέρειες. Θα έπρεπε να το ξέρω, ο αφελής. Τις προάλλες, στην Εβγα, μου το είπαν καθαρά. "Άνοιξε τα μάτια σου", μου είπανε. "Έχεις χάσει την επαφή σου με την κοινωνία."

Γι' αυτό, που λέτε, και συμφώνησα με την ιδέα να οργανώσουμε απόψε εκλογική βραδιά. Για να ξαναβρώ την επαφή μου με την κοινωνία.

Λοιπόν. Έχουμε μαζευτεί όλοι. Ο κύριος Κώστας με το καλώδιο είναι εδώ και πλέον έχουμε βίντεο. Έχουμε βάλει τις κασέτες να γυρίσουν στην αρχή, και περιμένουμε να σερβίρουμε την μπύρα ρυζιού με το που αρχίσουν τα έξιτ πολ.

Ελπίζω μόνο να λειτουργεί το fast forward.

Σας ασπάζομαι,
Θείος Ακάκιος


e-card
4000 1234 5678 9010
4000
GOOD THRU
MONTH / YEAR
12 / 19
MasterCard
Cardholder Name
Κάρτα e-coin, που δέχεται Bitcoins: Δουλεύει όπως όλες οι κανονικές κάρτες Debit, παντού στον κόσμο και για online αγορές.
Αποκτήστε τη δική σας με κλικ εδώ
και κερδίστε αυτομάτως
25% έκπτωση
κατά την παραγγελία της κάρτας.

Skill: Beginner
Tags: BitTorrent, TorGuard, OpenVPN, anonymity, privacy, DNS leaks, IPv6 leaks, WebRTC leaks, Stealth VPN, Deep Packet Inspection, killswitch

Στον αγώνα για ανέμελο torrenting, μέρος 1/3

Οι προδιαγραφές μιας ιδανικής λύσης και οι πρώτες δοκιμές

Πρόσφατα αντιμετωπίσαμε ένα περιστατικό που μας έκανε ν' αναθεωρήσουμε τη σχέση μας με το BitTorrent. Συνειδητοποιήσαμε ότι ακόμη κι ένας καλορυθμισμένος OpenVPN server, ο οποίος μάλιστα βρίσκεται υπό τον πλήρη έλεγχό μας, δεν είναι αρκετός για να ξεχάσουμε τα τελεσιγραφικά emails του στιλ "σταματήστε το κατέβασμα ή υποστείτε τις συνέπειες".

του Χρήστου Βαρελά

Οι τακτικοί αναγνώστες θα γνωρίζετε ίσως το θαυμασμό που τρέφουμε προς τη σύγχρονη κρυπτογραφία. Ειδικά για την προστασία των δικτυακών πακέτων που στέλνουμε και λαμβάνουμε από το Internet, συχνά προτιμάμε να τα δρομολογούμε μέσω ενός απομακρυσμένου OpenVPN server που εμείς οι ίδιοι έχουμε στήσει κι ελέγχουμε και συνεπώς τον εμπιστευόμαστε πλήρως. Κάθε φορά λοιπόν που βγαίνουμε στον έξω κόσμο κατ' αυτόν τον τρόπο, τα πακέτα που διακινούνται μεταξύ του υπολογιστή μας και του απομακρυσμένου server ταξιδεύουν μέσα από ένα ισχυρά κρυπτογραφημένο τούνελ και κανείς στο ενδιάμεσο δεν είναι σε θέση να τα διαβάζει – φυσικά ούτε ο ISP μας.

Τα προβλήματα αρχίζουν όταν βγαίνουμε από τον OpenVPN server, π.χ., για να επισκεφθούμε ένα web site, να χρησιμοποιήσουμε μια υπηρεσία streaming, να κατεβάσουμε κάτι κ.ο.κ. Μπορεί ο ISP μας να μη βλέπει τι κάνουμε, κάποια στιγμή όμως μοιραία αναδυόμαστε στο "κανονικό" Internet και η δημόσια διεύθυνση IP του OpenVPN server καταγράφεται. Αλλά για να μη μιλάμε γενικά, ας αναφερθούμε σε ένα πρόσφατο περιστατικό που βιώσαμε.

Ένα περιστατικό διαφορετικό από τα άλλα

Μεταξύ των διαφόρων άρθρων που κατά καιρούς έχουμε δημοσιεύσει περί OpenVPN, στο τεύχος 048 (https://deltahacker.gr/deltahacker048) δείξαμε πόσο εύκολο είναι να εγκαταστήσουμε τον δικό μας Access Server σε VPS

στο cloud (https://deltahacker.gr/?p=15064). Σε άλλο άρθρο του ίδιου τεύχους πήγαμε το θέμα λίγο παρακάτω και ρυθμίσαμε έναν pfSense-based router ώστε να λειτουργεί ως client για τον συγκεκριμένο OpenVPN Access Server (https://deltahacker.gr/?p=15109). Κατ' αυτόν τον τρόπο είναι πολύ εύκολο να ορίζουμε κανόνες (https://deltahacker.gr/?p=15323) για το ποια μηχανήματα του τοπικού δικτύου βγαίνουν στον έξω κόσμο μέσω OpenVPN και ποια όχι, κανόνες για τις μέρες της εβδομάδας ή/και για τις ώρες της ημέρας που η κίνηση ενός host δρομολογείται μέσω OpenVPN κ.ο.κ.

Ένα παρόμοιο setup υφίσταται και στο τοπικό δίκτυο της Parabing Creations, της μικρής εκδοτικής πίσω από το deltaHacker. Τις προάλλες, με τη βοήθεια του Transmission BitTorrent client κατεβάζαμε αμέριμνοι επεισόδια μιας σειράς που μας αρέσει κι όποτε έχουμε το χρόνο την παρακολουθούμε. Η εν λόγω σειρά δεν προβάλλεται από τα ελληνικά κανάλια ούτε διατίθεται μέσω Netflix (τουλάχιστον όχι για τη χώρα μας), οπότε άλλον τρόπο για να τη βλέπουμε δεν έχουμε. Το downloading των επεισοδίων έγινε μέσω OpenVPN Access Server που διατηρούμε σε droplet της Digital Ocean, σε datacenter στο New Jersey (η εταιρεία ονομάζει τα VPS της "droplets"). Η αλήθεια είναι ότι από τη στιγμή που το droplet κατοικεί σε αμερικάνικο έδαφος, δεν θα έπρεπε να κατεβάζουμε μέσω αυτού. Αλλά ξέρετε τι πανίσχυρο τέρας είναι η συνήθεια, ειδικά όταν υποβοηθείται από τις δυνάμεις του Σιγά-Μωρέ-Μη-Συμβεί-Σ'-Εμένα (TM).

Γύρω στις 48 ώρες μετά το downloading, οι δυνάμεις του Σιγά-Μωρέ-Μη-Συμβεί-Σ'-Εμένα (TM) γελούσαν εις βάρος μας – μερικές μάλιστα είχαν πέσει στο πάτωμα και δυσκολεύονταν ν' ανασάνουν. Στο inbox του προσωπικού mail server του γράφοντα (https://deltahacker.gr/?p=14096) είχε καταφθάσει email από τη Digital Ocean. Αφήνοντας στην άκρη τα τυπικά, η ουσία του email είχε ως ακολούθως:

```
Δεχθήκαμε παράπονα από την τάδε σύμπραξη κατόχων πνευματικών δικαιωμάτων επί ταινιών/σειρών/μουσικής. Από αυτή τη διεύθυνση IP, η οποία είναι από το δίκτυό μας και την έχει το droplet σας, κάποιος πραγματοποίησε downloading μέσω BitTorrent εκείνου και τ' άλλου αρχείου. Η λήψη έλαβε χώρα από εκείνη έως και την άλλη την ώρα, της δείνα ημερομηνίας. Τα αρχεία σχετίζονται με υλικό που προστατεύεται από πνευματικά δικαιώματα. Παρακαλείσθε όπως τα διαγράψετε αμέσως. Παροτρύνεστε επίσης να προβείτε στις κατάλληλες ενέργειες, ώστε να μην παρατηρηθεί ξανά παρόμοια δραστηριότητα από το λογαριασμό σας. Σε περίπτωση που αποτύχετε να συμμορφωθείτε διατηρούμε το δικαίωμα για μόνιμο κλείσιμο του λογαριασμού σας. Ευχαριστούμε για τη συνεργασία, χαρείτε τη μέρα σας.
```

Ομολογούμε πως δεν είναι η πρώτη φορά που λαμβάνουμε παρόμοιο email. Πριν τέσσερα περίπου χρόνια συντηρούσαμε ένα Tor exit node σε BSD VM, κάπου στην Καλιφόρνια. Ο VM provider είχε τραμπουκιστεί από την MPAA και με τη σειρά του τραμπούκισε εμάς. Ουσιαστικά, κάποιοι αθεόφοβοι επιβάρυναν το δίκτυο ανωνυμίας του Tor για το κατέβασμα ταινιών, σειρών κι ένας Θεός ξέρει τι άλλο. Υπεύθυνοι βέβαια φανήκαμε εμείς, αφού τρέχαμε exit node και το δημόσιο IP του αντίστοιχου VM καταγράφηκε από εκείνους που συμμετέχουν σε swarms μόνο και μόνο για να

παρακολουθούν ποιος κατεβάζει τι. Μετά το email που λάβαμε προσπαθήσαμε να δυσκολέψουμε τους downloaders, επιτρέποντας την έξοδο μόνο από συγκεκριμένα ports. Δεν καταφέραμε πολλά όμως. Αποφασίσαμε τελικά να συνεχίσουμε να στηρίζουμε το δίκτυο του Tor, αλλά με ένα απλό relay κι όχι με exit node.

Δύο χρόνια αργότερα επιχειρήσαμε να στήσουμε ξανά Tor exit node, αυτή τη φορά σε VPS που βρισκόταν σε datacenter λίγο έξω από το Ρέικιαβικ. Τους πρώτους μήνες όλα πήγαιναν καλά. Κάποια στιγμή όμως ένας administrator από Ιαπωνία (ή ήταν από Κορέα;) έστειλε email στον VPS provider, επισημαίνοντας ότι ένα από τα VPS του παρουσίαζε συμπεριφορά χαρακτηριστική ενός malware. Σ(ι)ούρ ινάφ, επρόκειτο για το VPS μας και, κάπως έτσι, άλλος ένας exit node μετατράπηκε σε απλό relay.

Αυτή τη φορά, με το email της Digital Ocean, η κατάσταση είχε μια σημαντική διαφορά σε σύγκριση με τις άλλες δύο: Οι υπεύθυνοι για την αναστάτωση ήμασταν *πράγματι* εμείς κι όχι κάποιος βαριεστημένος λογιστής από το Μπόουζμαν της Μοντάνα, ούτε ένας ζωηρός uber-haxxor-wannabe από το Ντίλι του Ανατολικού Τιμόρ. Απαντήσαμε αμέσως στη Digital Ocean ευχαριστώντας τους για την ενημέρωση, τους εξηγήσαμε ότι θα διερευνήσουμε το ζήτημα και θα βρούμε τον υπεύθυνο, ενώ τους υποσχεθήκαμε ότι αυτή η συμπεριφορά δεν θα επαναληφθεί. Μάλλον δεν μας πίστεψαν, απάντησαν ωστόσο ευγενικά ευχαριστώντας μας που τους ευχαριστήσαμε – βεβαίως και που συμμορφωθήκαμε προς τας υποδείξεις.

Είναι προφανές ότι η χρήση του *συγκεκριμένου* OpenVPN Access Server για το κατέβασμα περιεχομένου που προστατεύεται από πνευματικά δικαιώματα, αποτέλεσε τουλάχιστον αφελή ενέργεια από μέρους μας. Αν θέλουμε να προστατεύουμε την ιδιωτικότητά μας και ταυτόχρονα να κάνουμε και το περιστασιακό μας torrenting, τότε χρειαζόμαστε εναλλακτική προσέγγιση.

Αναζητώντας τον ιδανικό VPN provider

Το κατέβασμα μέσω BitTorrent δεν πρέπει να είναι ανιχνεύσιμο από τον ISP μας, κι αυτό διασφαλίζεται σχετικά εύκολα χάρη στο VPN tunneling. Το περιστατικό εξάλλου με τον Access Server και τη Digital Ocean, αποδεικνύει ότι εκτός από τον ISP έχουμε ν' ανησυχούμε και για τον VPN provider: η ταυτότητά μας πρέπει να του είναι άγνωστη. Μαζί με το privacy ως προς τον ISP, λοιπόν, χρειαζόμαστε *και* anonymity ως προς τον VPN provider. Είναι επίσης επιθυμητή η δυνατότητα επιλογής της γεωγραφικής περιοχής όπου βρίσκεται ο VPN server. Έτσι, αναλόγως της επιλογής μας τη μία φορά θα φαίνεται ότι βρισκόμαστε στο Νησί του Πάσχα, την άλλη στην Ελβετία, την παράλλη στο Άινταχο κ.ο.κ. Φυσικά, το να στήσουμε ένα σωρό OpenVPN servers σε datacenters εδώ κι εκεί στον πλανήτη, δεν αυξάνει απότομα μόνο τη δυσκολία διαχείρισης αλλά και το κόστος. Αυτό που θα θέλαμε είναι *έναν* VPN provider, ο οποίος με χαμηλό κόστος θα μας επιτρέπει να επιλέγουμε "σημείο εξόδου".

Καθώς κάναμε τη σύντομη λίστα με τις προδιαγραφές μιας λύσης για ασφαλές torrenting, θυμηθήκαμε μια είδηση που είχαμε διαβάσει στο site του περιοδικού (https://deltahacker.gr/?p=13298). Επρόκειτο για έρευνα που είχε διεξαγάγει το TorrentFreak, επιχειρώντας να καταγράψει την πολιτική των VPN providers ως προς τη διατήρηση αρχείων καταγραφής για την ταυτότητα αλλά και για τις δραστηριό-

τητες των πελατών τους. Όταν είχαμε πρωτοδιαβάσει το άρθρο, θετική εντύπωση μάς είχε κάνει το TorGuard. Από την πρώτη φορά που η ομώνυμη υπηρεσία μπήκε στο ραντάρ μας, έχουμε διαβάσει πολλά θετικά σχόλια γι' αυτή. Αποφασίσαμε, λοιπόν, ότι έχει φτάσει η ώρα να τη δοκιμάσουμε στην πράξη.

Υπηρεσία VPN για τους φίλους του BitTorrent

Το όνομα TorGuard (https://torguard.net) παραπέμπει στο σύστημα ανωνυμίας του Tor, στην πραγματικότητα όμως το "Tor" αποτελεί αναφορά στο torrent. Η εταιρεία δεν κρύβει ότι απευθύνεται στους χρήστες εφαρμογών BitTorrent, παρέχοντας λύσεις για τη διασφάλιση της ανωνυμίας τους. Αναλυτικότερα, με την υπηρεσία Anonymous Proxy ο πελάτης ρυθμίζει *μεμονωμένες* εφαρμογές ώστε να χρησιμοποιούν ανώνυμους διαμεσολαβητές. Από την άλλη, με την υπηρεσία Anonymous VPN οι υπολογιστές μας και *όλες* οι εφαρμογές που τρέχουν είναι δυνατόν να έχουν ανώνυμη αλλά και κρυπτογραφημένη πρόσβαση σε πλήθος VPN servers της εταιρείας ανά τον πλανήτη. Σημειώστε ότι επιτρέπεται να συνδέουμε έως και πέντε συσκευές μας στους servers του TorGuard. Αν όμως διαθέτουμε έναν router ο οποίος μπορεί να λειτουργεί ως OpenVPN client, τότε όλες οι συσκευές πίσω του είναι δυνατόν να βγαίνουν στο Internet από τους VPN servers της εταιρείας.

Το κλειδί σε κάθε περίπτωση είναι η ανωνυμία, συγκεκριμένα η υπόσχεση για μη τήρηση αρχείων καταγραφής για τους πελάτες του TorGuard. Όποτε η εταιρεία λαμβάνει ειδοποιήσεις για παραβίαση πνευματικών δικαιωμάτων, απλά *αδυνατεί* να γνωρίζει ποιοι είναι οι χρήστες που με τη δραστηριότητά τους παραβίασαν τα όποια δικαιώματα. Το δε σύστημα πληρωμών της εταιρείας είναι σε διαφορετικό δίκτυο από εκείνο με τους proxies και τους VPN servers, ενώ υπάρχει και δυνατότητα πληρωμής μέσω BitCoin. Έτσι, η ταυτότητα των πελατών προστατεύεται ακόμα περισσότερο.

Από τις δύο υπηρεσίες που παρέχονται για τη διασφάλιση της ανωνυμίας επιλέξαμε την Anonymous VPS, αφού εκτός από την ανωνυμία μας ενδιαφέρει *και* η ιδιωτικότητα (privacy). Για την υλοποίηση κρυπτογραφημένων τούνελ το TorGuard επιστρατεύει τη δοκιμασμένη τεχνολογία του OpenVPN και υπάρχουν σχετικοί servers σε περισσότερες από 65 γεωγραφικές περιοχές ανά τον πλανήτη. Φυσικά, ο πελάτης έχει τη δυνατότητα για επιλογή OpenVPN server. Αναλόγως λοιπόν της δραστηριότητάς του, δύναται να βγαίνει στο Internet από χώρες που είναι φιλικές ως προς το privacy ή από servers μέσω των οποίων θα έχει ανεμπόδιστη πρόσβαση σε υπηρεσίες όπως το Netflix.

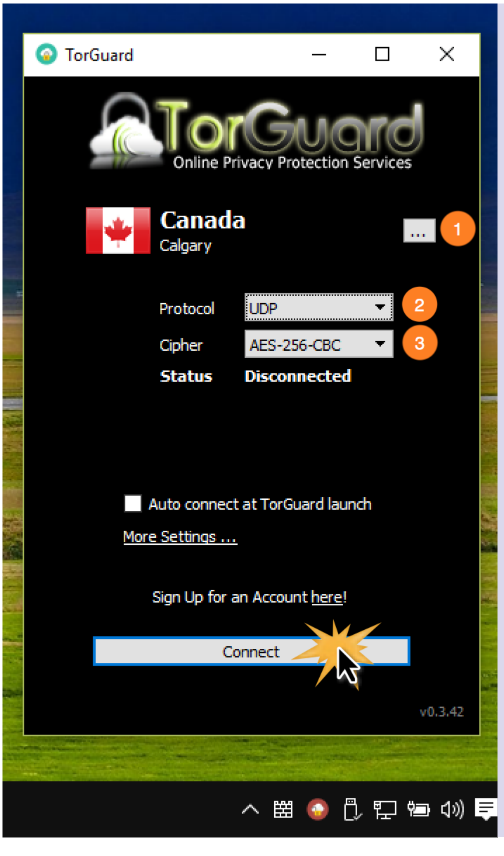
Σημείωση. Το Netflix έχει αρχίσει να διατίθεται παντού στον πλανήτη, ωστόσο δεν παρέχεται το ίδιο περιεχόμενο σε κάθε χώρα. Ο πιο πλούσιος κατάλογος είναι διαθέσιμος στην Αμερική και η Netflix έχει ανακοινώσει πως θα κάνει ό,τι μπορεί, ώστε να εμποδίζει τους πελάτες που χρησιμοποιούν proxies ή VPN servers. Η TorGuard δεν άργησε ν' απαντήσει. Υποσχέθηκε ότι θα προσθέτει διαρκώς νέους servers, ώστε οι πελάτες της, αν κι όποτε το επιθυμούν, να συνεχίσουν να έχουν πρόσβαση *και* στο περιεχόμενο του αμερικάνικου Netflix.

Πώς ξεκινάμε με το Anonymous VPN;

Παρέχονται μηνιαία, τρίμηνα, εξάμηνα κι ετήσια πακέτα. Το ετήσιο βγαίνει στα 5 δολάρια ανά μήνα, όσο δηλαδή και το πιο φθηνό droplet της Digital Ocean. Προτείνουμε να ξεκινήσετε με το μηνιαίο πακέτο, ώστε να δείτε αν η υπηρεσία σάς κάνει. Θα πληρώσετε 9,99 δολάρια αλλά τουλάχιστον θα έχετε την άνεση του χρόνου για να δοκιμάσετε το TorGuard στην πράξη, καθώς και να παίξετε με διάφορα configurations (γι' αυτά συζητάμε στα επόμενα μέρη του αφιερώματός μας). Αν για οποιονδήποτε λόγο αποφασίσετε ότι η υπηρεσία Anonymous VPN του TorGuard δεν σας κάνει ή απλά δεν είστε έτοιμος για συνδρομή, μην ξεχάσετε να ακυρώσετε την τρέχουσα: κάντε login στο client dashboard, μετά πάνω στο όνομα της υπηρεσίας σας, ύστερα στο κουμπάκι Management Actions κι επιλέξτε το Request Cancellation.

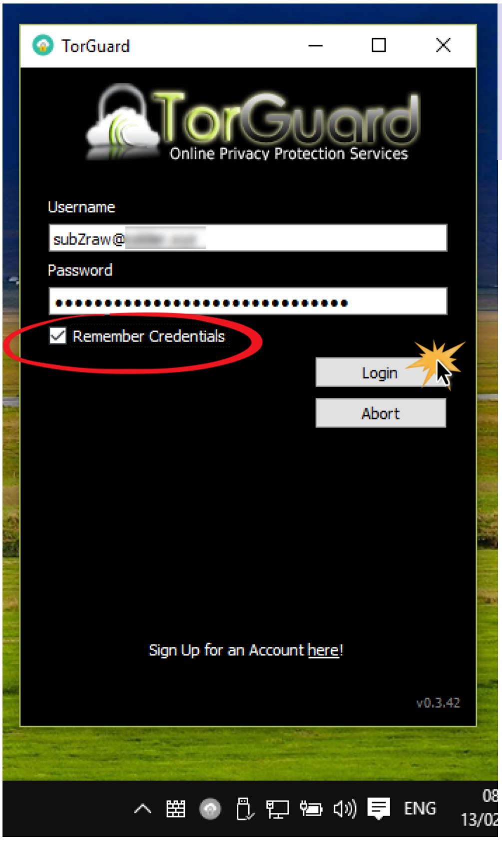
Δυνατότητες σύνδεσης

Από τη σελίδα https://torguard.net/downloads.php κατεβάζουμε το TorGuard lite VPN app, για το λειτουργικό σύστημα της προτίμησής μας (Linux, Windows, OS X). Για τη σύνδεση σε κάποιον OpenVPN server θα χρειαστεί να πληκτρολογήσουμε το username και το password μας στην υπηρεσία, όπως τα καθορίσαμε κατά την εγγραφή μας.

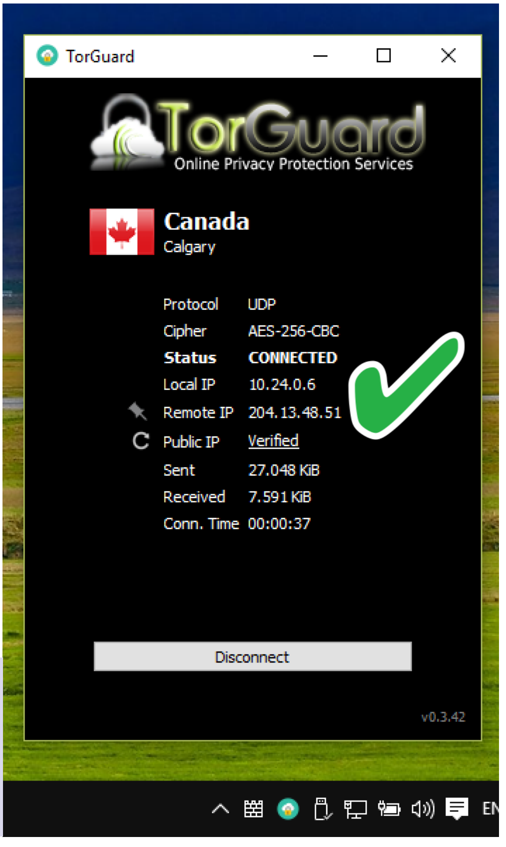


*Πριν την πραγματοποίηση μιας σύνδεσης έχουμε δυνατότητα επιλογής απομακρυσμένου OpenVPN server. Στο παράδειγμα έχουμε ξεχωρίσει έναν server στο Calgary του Καναδά (1). Για το πρωτόκολλο μεταφοράς πάνω από το οποίο υλοποιείται το κρυπτογραφημένο τούνελ, οι δυνατότητες είναι δύο: TCP ή UDP (2). Το TCP το προτιμάμε αν μας ενδιαφέρει η αξιοπιστία, αφού το πρωτόκολλο εγγυάται την παράδοση των πακέτων. Επίσης, τα VPN τούνελ πάνω από TCP χρησιμοποιούν τυπικά ports, όπως το 80 ή το 443, συνεπώς σπανίως μπλοκάρονται. Αν πάλι πρώτο μας μέλημα είναι η ταχύτητα, π.χ., λόγω εφαρμογών streaming, P2P, torrenting κ.ο.κ., τότε προτείνεται να επιλέγουμε το UDP. Σε αντίθεση με το TCP, το πρωτόκολλο UDP δεν εγγυάται την παράδοση των πακέτων κι επομένως οι συνδέσεις πάνω απ' αυτό είναι λιγότερο αξιόπιστες. Στην πράξη πάντως σπανίως θα έχουμε προβλήματα. Παρέχεται εξάλλου δυνατότητα για επιλογή του αλγορίθμου κρυπτογράφησης (cipher) (3). Ο AES-256-CBC προσφέρει τη μέγιστη δυνατή ασφάλεια, αλλά σε κάποιες περιπτώσεις έχει μια κάποια αρνητική επίπτωση στην ταχύτητα. Για πολύ καλό επίπεδο ασφάλειας αλλά *και* ταχύτητα, προτείνεται ο AES-128-CBC. Το TorGuard υποστηρίζει και τον Blowfish cipher (BF-CBC), ωστόσο για αυξημένες επιδόσεις και ασφάλεια καλό είναι να επιλέγουμε τον AES-128-CBC. Αν, τέλος, θέσουμε Cipher = None, τότε η σύνδεσή μας προς τον απομακρυσμένο OpenVPN server δεν θα είναι κρυπτογραφημένη. Αναλυτικότερα: Τα στοιχεία του λογαριασμού μας (username και password) μεταδίδονται κρυπτογραφημένα, η διεύθυνση IP που μας έχει δώσει ο ISP παραμένει κρυμμένη (βγαίνουμε στο Internet με το δημόσιο IP του απομακρυσμένου OpenVPN server), ωστόσο μεταξύ του client και του server δεν υφίσταται κρυπτογραφημένο τούνελ κι έτσι*

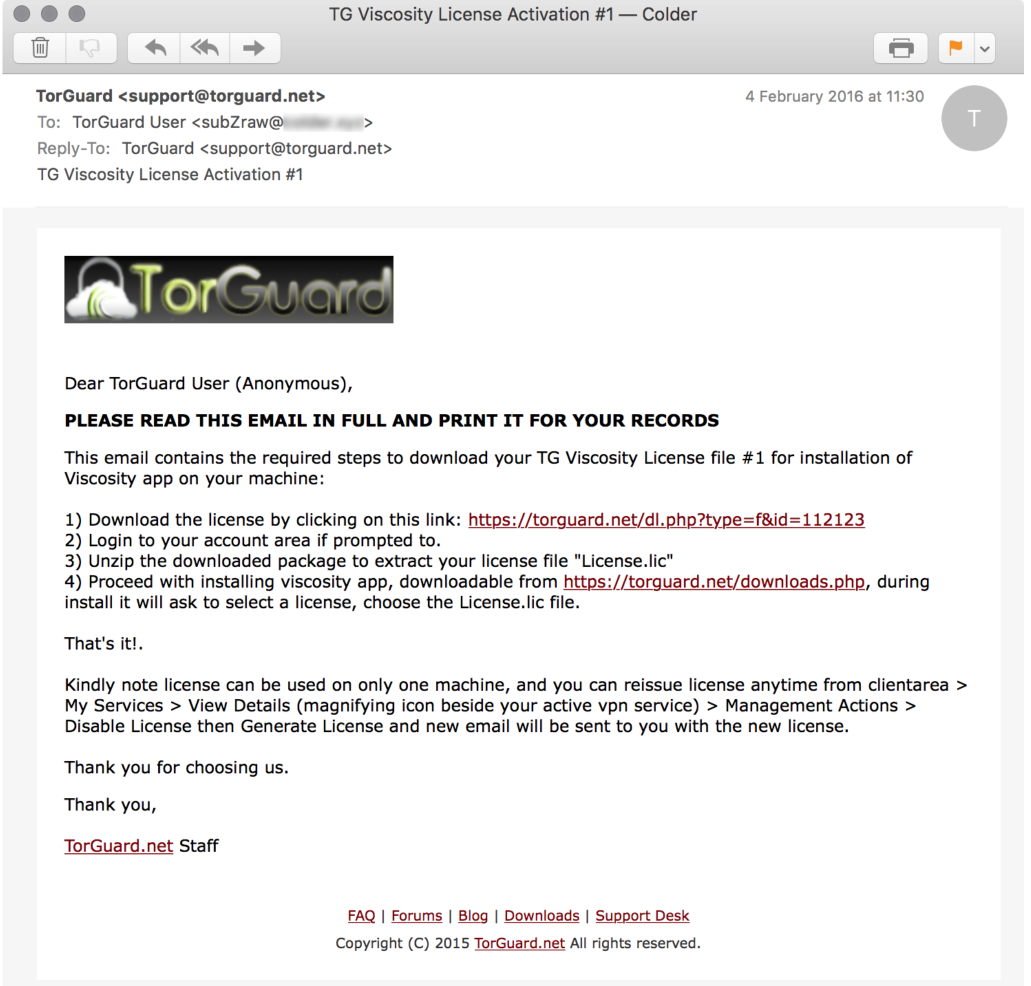
ο ISP μας είναι σε θέση να βλέπει τη δικτυακή μας δραστηριότητα. Θέτουμε Cipher = None όταν και μόνον όταν θέλουμε να κρύβουμε την ταυτότητά μας, μας ενδιαφέρει να έχουμε τη μέγιστη δυνατή ταχύτητα σύνδεσης προς τον OpenVPN server, ενώ την ίδια στιγμή δεν μας ενδιαφέρει το τι βλέπει ο ISP μας.



Αφού δώσουμε τα credentials του λογαριασμού μας (username και password) στο TorGuard lite VPN app, καλό είναι να τσεκάρουμε και το κουτάκι Remember Credentials. Έτσι, δεν θα χρειάζεται να τα πληκτρολογούμε κάθε φορά που θα επιχειρούμε σύνδεση.



Μετά την επίτευξη σύνδεσης το TorGuard lite VPN app παρουσιάζει τη διεύθυνση του tunnel interface (Local IP), καθώς και τη διεύθυνση με την οποία βγαίνουμε στο Internet (Remote IP). Κατά περιπτώσεις, είναι λογικό να θέλουμε να κάνουμε μερικούς έξτρα ελέγχους, μόνοι μας. Περισσότερα επ' αυτού διαβάστε στην επόμενη παράγραφο.



TG Viscosity License Activation #1 — Colder

TorGuard <support@torguard.net>
To: TorGuard User <subZraw@[redacted]>
Reply-To: TorGuard <support@torguard.net>
TG Viscosity License Activation #1

4 February 2016 at 11:30

Dear TorGuard User (Anonymous),

PLEASE READ THIS EMAIL IN FULL AND PRINT IT FOR YOUR RECORDS

This email contains the required steps to download your TG Viscosity License file #1 for installation of Viscosity app on your machine:

1) Download the license by clicking on this link: https://torguard.net/dl.php?type=f&id=112123
2) Login to your account area if prompted to.
3) Unzip the downloaded package to extract your license file "License.lic"
4) Proceed with installing viscosity app, downloadable from https://torguard.net/downloads.php, during install it will ask to select a license, choose the License.lic file.

That's it!.

Kindly note license can be used on only one machine, and you can reissue license anytime from clientarea > My Services > View Details (magnifying icon beside your active vpn service) > Management Actions > Disable License then Generate License and new email will be sent to you with the new license.

Thank you for choosing us.

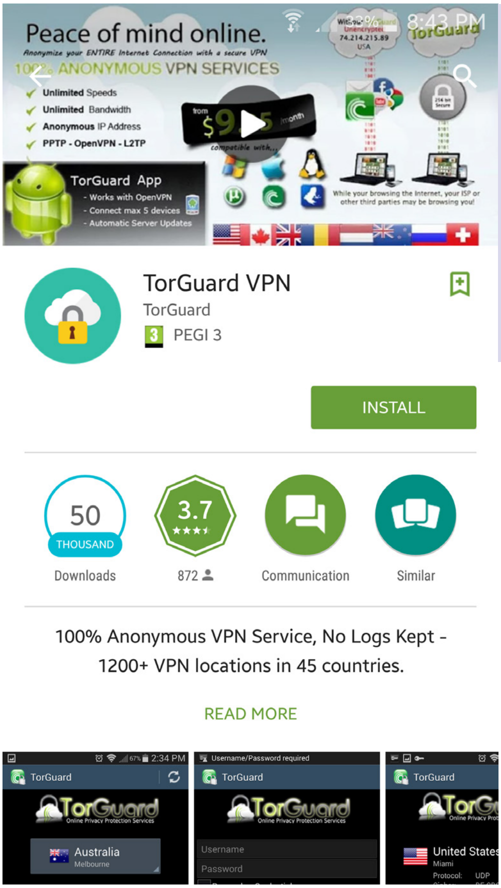
Thank you,

TorGuard.net Staff

FAQ | Forums | Blog | Downloads | Support Desk

Copyright (C) 2015 TorGuard.net All rights reserved.

Οι πελάτες του TorGuard λαμβάνουν δωρεάν άδεια χρήσης για τον εμπορικό OpenVPN client ονόματι Viscosity, ο οποίος διατίθεται για Windows και OS X (https://www.sparklabs.com/viscosity). Το Viscosity κοστίζει εννέα δολάρια και είναι ο αγαπημένος μας OpenVPN client προς τους δικούς μας OpenVPN servers. Για την περίπτωση όμως του TorGuard, δεν βλέπουμε το λόγο να προτιμήσουμε το Viscosity έναντι του TorGuard lite VPN app. Αντίθετα, στο προαναφερθέν βλέπουμε προτερήματα που δεν έχει το Viscosity. Κατ' αρχάς, το TorGuard lite VPN app το εγκαθιστούμε σε όσα μηχανήματα θέλουμε, ενώ για το Viscosity κανονικά προβλέπεται μία εγκατάσταση ανά άδεια χρήσης. Αλλά η πιο σημαντική διαφοροποίηση έγκειται στα killswitches και Stealth VPN, δύο σημαντικές δυνατότητες που παρέχει μόνο το TorGuard lite VPN app. Περισσότερα επ' αυτών στη συνέχεια του παρόντος άρθρου.



Εφαρμογές για σύνδεση στους OpenVPN servers του TorGuard διατίθενται τόσο για Android όσο και για iOS. Είναι δωρεάν, όμως για τη σύνδεση χρειάζονται τα credentials λογαριασμού με ενεργή συνδρομή. Δεν έχουμε λόγο για χρήση OpenVPN στο smartphone, εγκαταστήσαμε ωστόσο τον επίσημο client για Android και παίξαμε λίγο. Παρατηρήσαμε ότι για την κρυπτογράφηση χρησιμοποιούταν ο Blowfish cipher και δεν υπήρχε δυνατότητα για χρήση AES-128 ή AES-256. Λογικά πρόκειται για συνειδητή επιλογή των προγραμματιστών της εφαρμογής, ώστε να μην επιβαρύνεται η μπαταρία της συσκευής. Κατά τα άλλα, ο χρήστης του app επιλέγει μεταξύ των OpenVPN servers που έχει η εταιρεία ανά τον πλανήτη και οι συνδέσεις πραγματοποιούνται επιτυχώς.

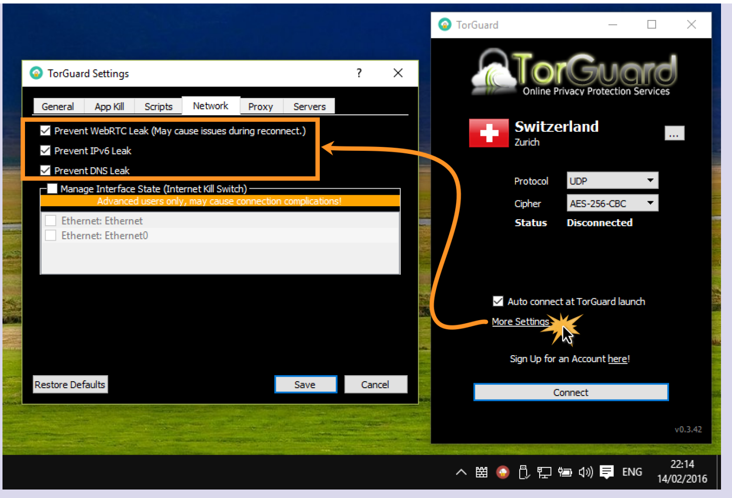
Στους servers του TorGuard μπορούμε να συνδεόμαστε κι από το "κλασικό" Unix-οειδές OpenVPN, ζητώντας του να συμπεριφερθεί ως απλός client. Χρειαζόμαστε βέβαια τα απαραίτητα πιστοποιητικά και configuration files, τα οποία λαμβάνουμε από το site του TorGuard. Αν πάλι ο router μας υποστηρίζει λειτουργικότητα OpenVPN client, τότε μπορούμε να συνδέσουμε εκείνον στους servers του TorGuard. Περισσότερα για όλα αυτά διαβάστε στα δύο επόμενα μέρη του αφιερώματός μας, τα οποία ξεκινούν από τις σελίδες 40 και 72.

Δοκιμές και έλεγχοι

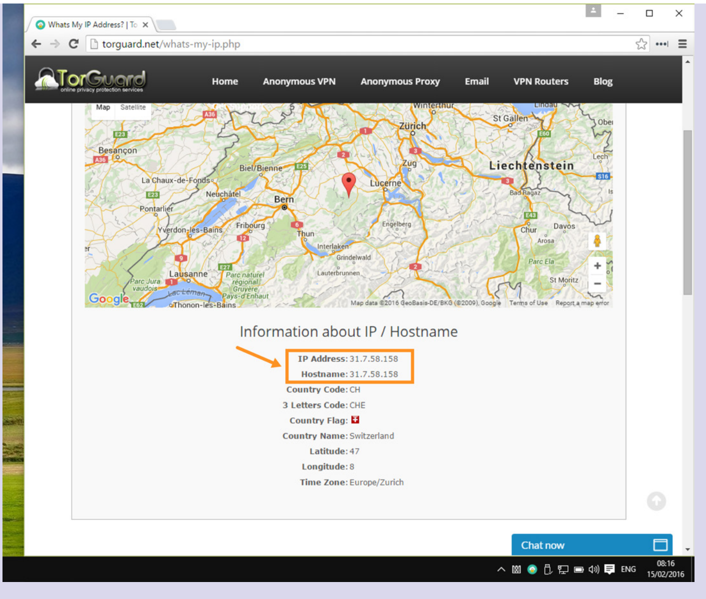
Θέλουμε να βεβαιωθούμε για τα ακόλουθα:

- στο Internet εμφανιζόμαστε με το δημόσιο IP του εκάστοτε OpenVPN server κι όχι με εκείνο που μας έχει δώσει ο ISP μας
- χρησιμοποιούμε τους name servers που υποδεικνύει ο OpenVPN server κι όχι εκείνους του ISP
- κατά το κατέβασμα torrents, η δημόσια διεύθυνση IP από τον ISP *δεν* διαρρέει
- είμαστε προστατευμένοι ως προς το ύπουλο WebRTC leak (βλ. παρακάτω).

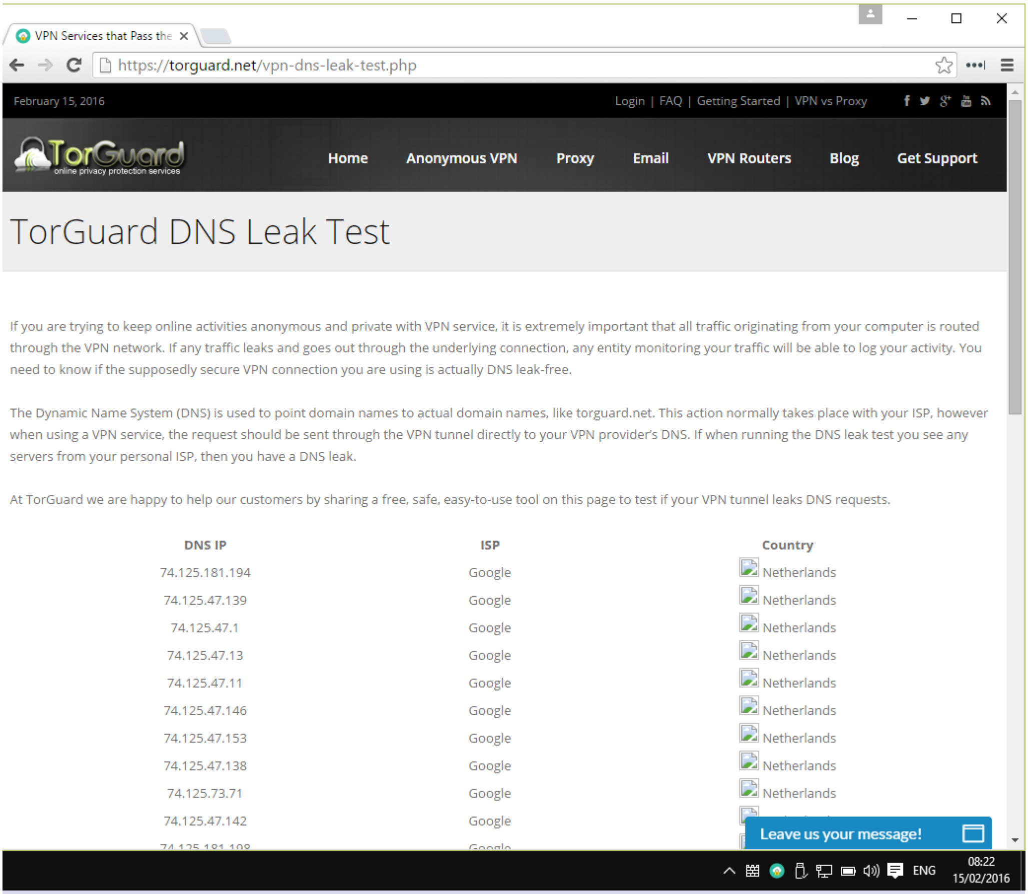
Τις δικές μας δοκιμές τις κάναμε από ένα μηχάνημα με Windows 10, χρησιμοποιώντας το TorGuard lite VPN app. Δείτε τα screenshots που ακολουθούν κι οπωσδήποτε διαβάστε τις αντίστοιχες περιγραφές.



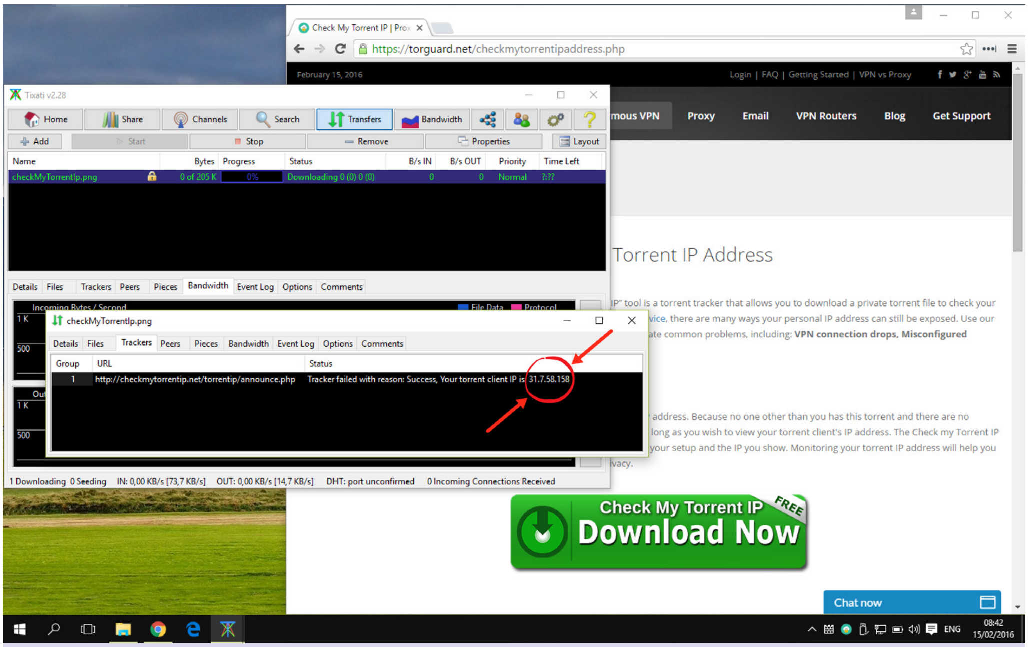
Πριν την όποια δοκιμή, για την ακρίβεια πριν τη σύνδεση σε κάποιον OpenVPN server, επισκεπτόμαστε τις ρυθμίσεις του TorGuard lite VPN app και συγκεκριμένα την καρτέλα Network. Εκεί, φροντίζουμε ώστε τα κουτάκια Prevent WebRTC Leak, Prevent IPv6 Leak και Prevent DNS Leak να είναι όλα τσεκαρισμένα. Στη συνέχεια συνδεόμαστε σε κάποιον από τους OpenVPN servers του TorGuard. Εμείς συνδεθήκαμε σε έναν που βρίσκεται στη Ζυρίχη.



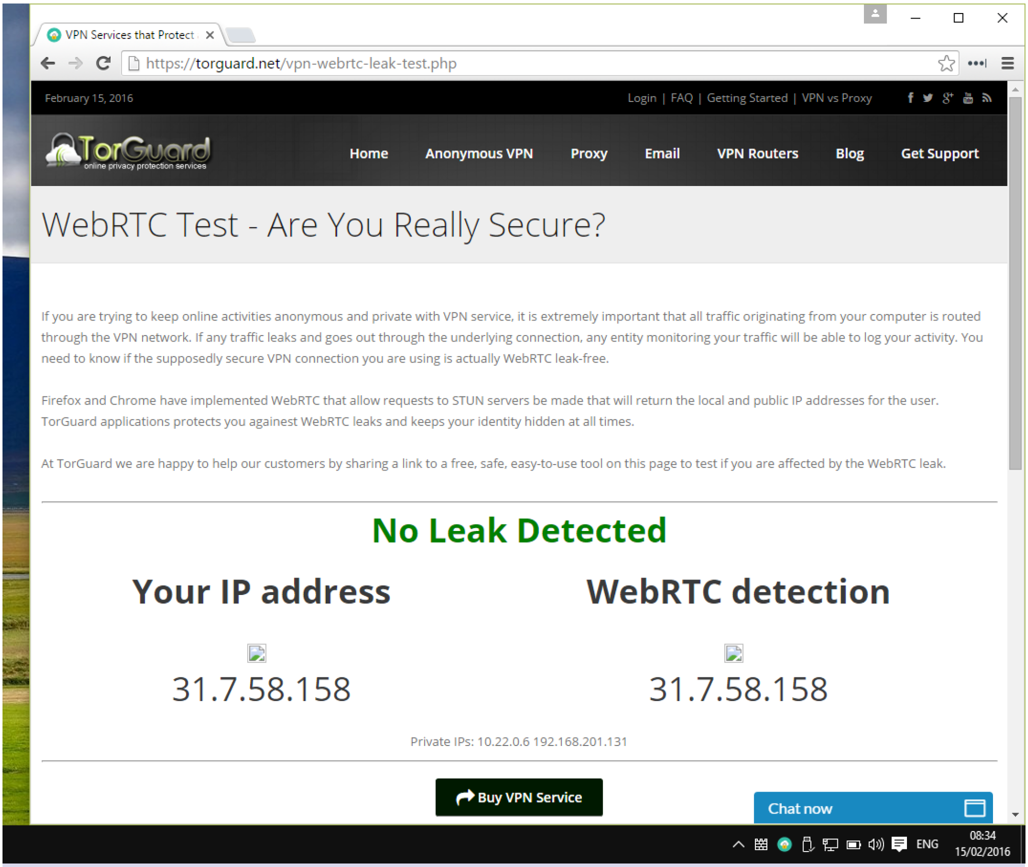
Για τον έλεγχο της δημόσιας διεύθυνσης IP με την οποία βγαίνουμε στο Internet, το TorGuard προτείνει να επισκεφθούμε τη διεύθυνση http://torguard.net/whats-my-ip.php – βεβαίως από τον web browser της προτίμησής μας. Δεν είναι υποχρεωτικό να πάμε σ' αυτή τη διεύθυνση. Υπάρχει μια πληθώρα sites που εμφανίζουν στον browser το δημόσιο IP μας (το http://ifconfig.me είν' ένα από αυτά). Ακόμη και μια αναζήτηση του στιλ "what is my ip" να κάνουμε στο Google, το πρώτο αποτέλεσμα που θα επιστρέψει η μηχανή θα είναι το δημόσιο IP μας. Σε κάθε περίπτωση, από τη στιγμή που είμαστε συνδεδεμένοι σε OpenVPN server, το εν λόγω IP θα πρέπει να είναι διαφορετικό από εκείνο που μας έχει δώσει ο ISP μας. Αν δεν είσαστε βέβαιοι για το προαναφερθέν, αποσυνδεθείτε από τον OpenVPN server κι ακολούθως αναζητήστε το IP με κάποιους από τους τρόπους που μόλις αναφέραμε.



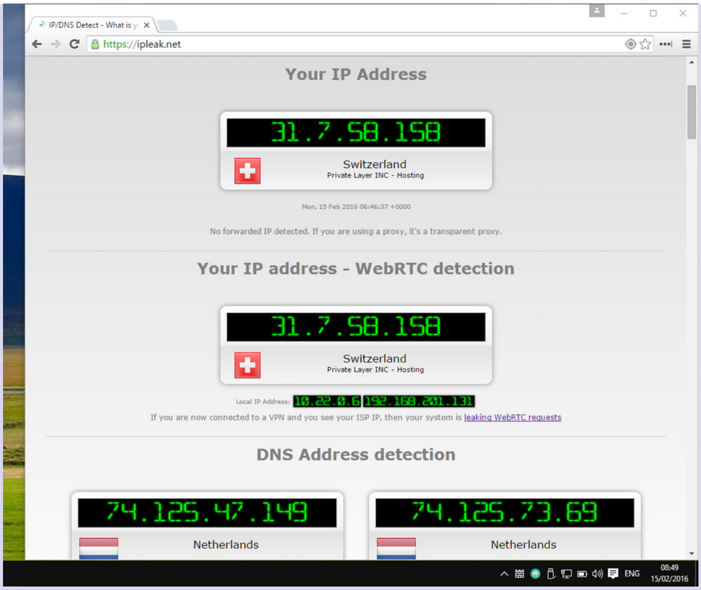
Όταν είμαστε συνδεδεμένοι σε απομακρυσμένο OpenVPN server αλλά τα DNS queries απαντώνται από κάποιον name server του ISP μας ή, γενικότερα, από κάποιον name server του τοπικού σημείου σύνδεσης στο Internet (π.χ., δημόσιο Hotspot, WiFi καφετέριας, ξενοδοχείου κ.λπ.), τότε έχουμε DNS leak και η ιδιωτικότητά μας υποβαθμίζεται. Πράγματι, ενώ τα πακέτα που στέλνουμε και λαμβάνουμε παραμένουν κρυπτογραφημένα, κάποιος τρίτος είναι σε θέση να βλέπει ποια sites επισκεπτόμαστε, ποιες υπηρεσίες χρησιμοποιούμε κ.ο.κ. Οι OpenVPN servers του TorGuard είναι έτσι ρυθμισμένοι ώστε να ενημερώνουν τους πελάτες για τους δικούς τους name servers. Μολαταύτα, σε κάποιες περιπτώσεις ακόμη και τότε είναι πιθανό να έχουμε DNS leak. Στα Windows, π.χ., όπου δεν υπάρχει η έννοια του καθολικού name server, κάθε δικτυακό ενδιάμεσο (network interface) επιτρέπεται να έχει τον δικό του name server. Σε κάποιες περιπτώσεις το λειτουργικό αγνοεί το routing table και την προκαθορισμένη πύλη, συνεπώς τα DNS queries δεν αποστέλλονται μέσω του tunneling interface κι έχουμε DNS leak. Ανεξαρτήτως του λειτουργικού συστήματος που χρησιμοποιούμε, προκειμένου να ελέγξουμε αν το σύστημά μας παρουσιάζει DNS leaks μπορούμε απλά να επισκεφθούμε την ιστοσελίδα https://torguard.net/vpn-dns-leak-test.php. *Αν στους name servers που θα δούμε εκεί απουσιάζουν εκείνοι του ISP μας και του τοπικού δικτύου εντός του οποίου βρισκόμαστε, τότε δεν υπάρχει DNS leak. (Δεν έχουμε λόγο ανησυχίας αν οι name servers που ανιχνευτούν είναι εκείνοι της Google ή/και της OpenDNS.)*



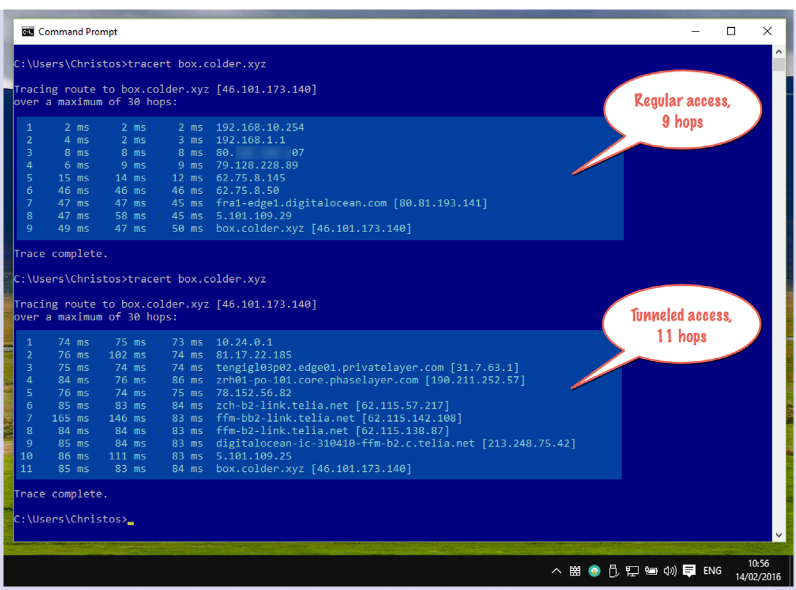
Ακόμη κι αν κατεβάζουμε torrents μέσω VPN, αυτό δεν σημαίνει ότι η διεύθυνση IP που έχουμε πάρει από τον ISP μας είναι αδύνατον να διαρρεύσει. Κάτι τέτοιο ίσως συμβεί εξαιτίας κάποιου ύπουλου bug στον BitTorrent client που χρησιμοποιούμε. Ίσως πάλι ο απομακρυσμένος OpenVPN πέσει, οπότε ξαφνικά θα βγαίνουμε στο Internet μέσω του ISP μας. Αν το όποιο τοπικό firewall επιτρέπει στον BitTorrent client να κατεβάζει μέσω μη-κρυπτογραφημένου network interface, τότε η δραστηριότητά μας ξαφνικά θα είναι ορατή στον ISP. Ένας τρόπος προκειμένου να βεβαιωθούμε για τη δημόσια διεύθυνση IP που έχουμε καθώς κατεβάζουμε κάποιο torrent με τον αγαπημένο μας client, είναι να πάμε πρώτα στη διεύθυνση https://torguard.net/checkmytorrentipaddress.php και να πάρουμε το torrent file που δίνεται από εκεί. Το συγκεκριμένο αρχείο θα το φορτώσουμε στον BitTorrent client της επιλογής μας. Δεν πρόκειται να κατέβει κάτι, στους trackers όμως θα δούμε το δημόσιο IP που έχει ο client. Αν είναι διαφορετικό από εκείνο που μας έχει δώσει ο ISP, τότε όλα είναι καλά. Αν *δεν* είναι διαφορετικό, βεβαιωνόμαστε κατ' αρχάς ότι η σύνδεσή μας προς το TorGuard είναι ενεργή. Ίσως επίσης χρειαστεί να ελέγξουμε και για διαθέσιμες ενημερώσεις για τον BitTorrent client. Για τις δοκιμές μας εμείς χρησιμοποιήσαμε το Tixati για Windows κι όλα πήγαν καλά. Επιτυχημένη δοκιμή κάναμε και με το Transmission για OS X. Στο δεύτερο άρθρο της σειράς μας, όπου στήνουμε ένα βολικό κι ασφαλές Seedbox, διασφαλίζουμε ότι όλα είναι καλά με τον BitTorrent client κι επιπρόσθετα φροντίζουμε ώστε να του μπλοκάρεται η πρόσβαση στο Internet, κάθε φορά που η σύνδεση προς τον OpenVPN server πέφτει.



Το WebRTC (Web Real-Time Configuration) είναι ένα API που δημιουργήθηκε από το World Wide Web Consortium (http://www.w3.org) κι επιτρέπει στους browsers να επικοινωνούν απευθείας για την υλοποίηση εφαρμογών chat, video calling, P2P filesharing κ.ά., χωρίς την ανάγκη για plugins. Πριν από έναν περίπου χρόνο το TorrentFreak αποκάλυψε ότι συγκεκριμένοι browsers που υποστηρίζουν το WebRTC πάσχουν από μια σοβαρή αδυναμία, η οποία οδηγεί στην κατάλυση της ασφάλειας των VPN tunnels μέσω της αποκάλυψης της δημόσιας διεύθυνσης IP που ο VPN client έχει πάρει από τον ISP. Μεταξύ άλλων browsers, η αδυναμία αφορά στους Firefox και Chrome και εκδηλώνεται κάτω από Windows. Το TorGuard lite VPN app για Windows παρέχει προστασία κατά του WebRTC leak. Από τις εκδόσεις για Linux και OS X η σχετική επιλογή απουσιάζει, αφού σ' αυτές τις πλατφόρμες το WebRTC leak δεν εκδηλώνεται. Προκειμένου να ελέγξουμε αν είμαστε ευάλωτοι ως προς το WebRTC leak bug, αρκεί να πάμε μια βόλτα από το https://diafygi.github.io/webrtc-ips ή από το https://torguard.net/vpn-webrtc-leak-test.php. Σε κάθε περίπτωση, το δημόσιο IP που έχουμε πάρει από τον ISP δεν πρέπει να ανιχνευθεί.



Για τους ελέγχους μας δεν είναι απαραίτητο να καταφεύγουμε στις σελίδες που προτείνει το TorGuard. Παράδειγμα: Από το https://ipleak.net έχουμε δυνατότητα ελέγχου για IP/DNS/WebRTC leaks, ενώ τσεκάρουμε και τη δημόσια διεύθυνση IP που εμφανίζει ο BitTorrent client της προτίμησής μας.



Ένα από τα κλασικά τεστ που μας αρέσει να κάνουμε, πριν και μετά τη σύνδεση σε OpenVPN server: Ανίχνευση της διαδρομής (traceroute) από το μηχάνημά μας έως συγκεκριμένο server στο Internet. Στο παράδειγμα, βρισκόμαστε σε ένα μηχάνημα με Windows 10 κι από ένα Command Prompt Window τρέχουμε το tracert για το box.colder.xyz.

Καταπολέμηση του Deep Packet Inspection και killswitches

Εφαρμόζοντας τεχνικές Deep Packet Inspection (DPI, https://en.wikipedia.org/wiki/Deep_packet_inspection) ένας ISP είναι εύκολο να διαπιστώνει αν οι πελάτες του χρησιμοποιούν κάποια τεχνολογία VPN. Σε ένα αγγελικά πλασμένο Internet, το DPI δεν θα απασχολούσε κανέναν πελάτη. Η πραγματικότητα όμως είναι λίγο διαφορετική. Για παράδειγμα, σε απολυταρχικά καθεστώτα το DPI εφαρμόζεται προκειμένου να επιτρέπεται ή να απαγορεύεται η πρόσβαση στο Internet για τους πολίτες. Αλλά και σε άλλες χώρες, συχνά το DPI επιστρατεύεται προκειμένου να αποθαρρύνεται η κρυπτογράφηση. Μπορεί, π.χ., κάποιος πελάτης να έχει αγοράσει σύνδεση στα 24Mbps, όταν όμως χρησιμοποιεί VPN tunneling ο ISP να του ελαττώνει την ταχύτητα στα 8Mbps (throttling).

Το TorGuard παρέχει τη δυνατότητα για το λεγόμενο Stealth VPN, κατά το οποίο τα κρυπτογραφημένα πακέτα μασκαρεύονται και δείχνουν ν' αποτελούν μέρος απλής κίνησης HTTPS. Η ιδέα είναι ότι οι τεχνικές DPI από πλευράς ISP θα αποτυγχάνουν να κατηγοριοποιούν τα πακέτα του χρήστη, συνεπώς δεν θα μπλοκάρεται η πρόσβασή του στο Internet, ούτε θα περιορίζεται η ταχύτητα σύνδεσής του. Το Stealth VPN δεν υποστηρίζεται από όλους τους OpenVPN servers του TorGuard, συνεπώς αν μας ενδιαφέρει τότε θα πρέπει να επιλέξουμε τον κατάλληλο server. Στη λίστα του TorGuard lite VPN app, οι υπό συζήτηση servers έχουν στα δεξιά τους ένα εικονίδιο που μοιάζει με οθόνη ραντάρ. Παρεμπιπτόντως, ο γεωγραφικά εγγύτερος Stealth VPN server που βρήκαμε ήταν στο Άμστερνταμ.

Να αναφέρουμε τέλος και τα killswitches, μια εξαιρετικά ενδιαφέρουσα αλλά και χρήσιμη δυνατότητα του TorGuard lite VPN app. Χάρη σ' αυτά, όταν για οποιονδήποτε λόγο χάνεται η σύνδεσή μας προς τον OpenVPN server, τότε μία ή περισσότερες εφαρμογές που εμείς έχουμε καθορίσει τερματίζονται αυτόματα. Σκεφτείτε, π.χ., ότι έχουμε αφήσει ένα μηχάνημα με Windows να κατεβάζει αμέριμνα, με χρήση του αγαπημένου μας BitTorrent client. Κάποια στιγμή ο απομακρυσμένος OpenVPN server εμφανίζει κάποιο πρόβλημα, με αποτέλεσμα η σύνδεσή μας προς αυτόν να διακοπεί. Τα Windows τότε θα συνεχίσουν να βγαίνουν στο Internet μέσω της κανονικής σύνδεσης προς τον ISP κι ο BitTorrent client θα συνεχίσει να κατεβάζει, προδίδοντας τη δραστηριότητά μας στον ISP. Θα γίνει, δηλαδή, ό,τι θέλαμε να αποφύγουμε – εκτός κι αν είχαμε φροντίσει να προσθέσουμε τον BitTorrent client στη λίστα των εφαρμογών που τερματίζονται κατά τη διακοπή της σύνδεσης VPN.

Στο δεύτερο άρθρο του αφιερώματος, που αρχίζει από τη σελίδα 40, δείχνουμε πώς φτιάχνουμε ένα ευέλικτο Seedbox με Ubuntu Server για ανέμελο κι ασφαλές torrenting. Στο τρίτο και τελευταίο άρθρο, που ξεκινά από τη σελίδα 72, ρυθμίζουμε κατάλληλα έναν pfSense-based router ώστε να διατηρεί ενεργές περισσότερες από μία συνδέσεις σε OpenVPN servers του TorGuard. Έτσι, η δικτυακή κίνηση ενός πλήθους μηχανημάτων πίσω από το pfSense θα προστατεύεται αποτελεσματικά – κι αναλόγως της βασικής αποστολής του αντίστοιχου μηχανήματος.

Skill: Beginner
Tags: Active Directory, Domain Controller, Linux, Kerberos, SMB, CIFS, Samba

Υπηρεσίες Active Directory, χωρίς active-τσέπη

[μέρος 1/2]

Η τεχνολογία Active Directory αποτελεί ευλογία™ για τα τοπικά δίκτυα με συστήματα που τρέχουν Windows. Σκεφτείτε τα μικρά εργαστήρια σχολείων και φροντιστηρίων ή ακόμα και τους χώρους εργασίας διαφόρων υπηρεσιών και άλλων φορέων. Καλά τα λέτε, θα σκεφτεί κανείς, μόνο που το Active Directory προϋποθέτει την παρουσία ενός Windows Server κι αυτό συνεπάγεται ένα καθόλου ευκαταφρόνητο κόστος. Ή μήπως όχι;

του Πέτρου Κυλαδίτη

Όσοι έχουν χρησιμοποιήσει συστήματα Windows που συνδέονται σε κάποιο Windows Domain, είναι πολύ πιθανό να έχουν γνωρίσει και εκτιμήσει τις λειτουργίες του Active Directory. Μια από τις ευκολίες που προσφέρει η συγκεκριμένη υπηρεσία σχετίζεται με τα λεγόμενα roaming profiles. Με απλά λόγια, ο εκάστοτε χρήστης μπορεί να κάθεται σε οποιοδήποτε μηχάνημα του δικτύου και μέσα σε ελάχιστο χρόνο να έχει μπροστά του το δικό του desktop, με τις δικές του ρυθμίσεις και τα δικά του αρχεία. Οι ευκολίες που προσφέρει το Active Directory μπορούν να αξιοποιηθούν από τις επαγγελματικές εκδόσεις των Windows και μόνον από αυτές. Με άλλα λόγια, από τις εκδόσεις που τιτλοφορούνται ως Professional/Enterprise/Ultimate κι όχι από εκείνες με το χαρακτηριστικό Home. Αυτές οι εκδόσεις του λειτουργικού της Microsoft μπορούν να συνδέονται σε Windows Domain και να απολαμβάνουν όλες τις προσφερόμενες ευκολίες. Οποιοσδήποτε πιστοποιημένος χρήστης του τομέα μπορεί να συνδεθεί σε οποιοδήποτε μηχάνημα–μέλος του τομέα κι από 'κει θα έχει πρόσβαση σε όλα τα δεδομένα του.

Στη ραχοκοκαλιά κάθε Windows Domain βρίσκεται ένα σύστημα που παίζει το ρόλο του διαχειριστή ή αλλιώς του domain controller. Οι υπολογιστές–μέλη του τομέα χρησιμοποιούν μια ειδική υπηρεσία αυτού του κεντρικού συστήματος, με τη βοήθεια της οποίας οι χρήστες πιστοποιούνται και εξακριβώνονται τα δικαιώματα πρόσβασης του καθενός. Η εν λόγω υπηρεσία προέρχεται από τη Microsoft και είναι κλειστού κώδικα, αν κι επί της ουσίας αποτελεί μια υλοποίηση του πρωτοκόλλου Kerberos, του MIT. Για το διαμοιρασμό των αρχείων επιστρατεύεται το γνωστό πρωτόκολλο SMB/CIFS.

SMB ή CIFS;

Το SMB προέρχεται από τα αρχικά Server Message Block και αποτελεί το όνομα ενός πρωτοκόλλου που αναπτύχθηκε από την IBM, στα μέσα της δεκαετίας του '80. Αποστολή του SMB ήταν η δυνατότητα εγγραφής κι ανάγνωσης κοινόχρηστων αρχείων, από υπολογιστές που βρίσκονται στο ίδιο τοπικό δίκτυο, ανεξάρτητα από το λειτουργικό σύστημα και το σύστημα αρχείων που υποστηρίζει ο καθένας. Από την άλλη, το CIFS προέρχεται από τα αρχικά Common Internet File System και αποτελεί την υλοποίηση του SMB από τη Microsoft. Με λίγα λόγια, το δεύτερο αποτελεί μια παραλλαγή του πρώτου. Σε ό,τι αφορά στις υπόλοιπες εφαρμογές ενός συστήματος, τα δύο πρωτόκολλα είναι πλήρως συμβατά.

Τα μηχανήματα που έχουν το ρόλο του domain controller χρησιμοποιούν μια ειδική εκδοχή του λειτουργικού της Microsoft, που ονομάζεται Windows Server. Η συγκεκριμένη εκδοχή προσφέρει όλες τις υπηρεσίες που αναφέραμε προηγουμένως, ενώ ενσωματώνει τον web server IIS, τον Microsoft SQL Server κ.ά. Όπως υποψιάζεστε, εκτός από τις διάφορες υπηρεσίες που, μεταξύ μας, δεν έχουν και την καλύτερη φήμη, το μεγαλύτερο μειονέκτημα του Windows Server είναι το υπέρογκο κόστος. Ως αποτέλεσμα, τοπικά δίκτυα που θα μπορούσαν να αξιοποιήσουν τις λειτουργίες του Active Directory, περιορίζονται στο μοντέλο των οικιακών ομάδων εργασίας και κάθε λογαριασμός χρήστη κατοικεί αποκλειστικά στο μικρόκοσμο του αντίστοιχου σταθμού εργασίας.

Δωρεάν εναλλακτική

Υπάρχει άραγε τρόπος να αξιοποιήσουμε την τεχνολογία Active Directory, χωρίς να επωμιστούμε το υπέρογκο κόστος του Windows Server; Η ερώτηση είναι προφανώς ρητορική, αλλιώς το παρόν άρθρο δεν θα είχε κανένα λόγο ύπαρξης.

Όπως αναφέραμε ήδη, για την πιστοποίηση των χρηστών χρησιμοποιείται μια έκδοση του πρωτοκόλλου Kerberos. Το εν λόγω πρωτόκολλο διατίθεται και από το MIT με άδεια χρήσης ελεύθερου λογισμικού κι εννοείται ότι υπάρχουν πακέτα για όλα τα συστήματα τύπου Unix, του Linux συμπεριλαμβανομένου. Με άδεια ανοιχτού κώδικα κυκλοφορεί και ο Samba server, που υλοποιεί το πρωτόκολλο δικτύωσης SMB, ενώ στις τελευταίες του εκδόσεις μπορεί ν' αναλάβει αξιόπιστα το ρόλο ενός domain controller. Τώρα καταλαβαίνετε πού το πάμε: Θα στήσουμε έναν domain controller με τη βοήθεια του Linux, για ένα δίκτυο με μηχανήματα που τρέχουν Windows.

Για τις ανάγκες του άρθρου στραφήκαμε στη διανομή Ubuntu Server, που θεωρείται ιδιαίτερα εύχρηστη και φιλική. Εξάλλου, η απουσία οποιουδήποτε περιβάλλοντος γραφικών, κάτι παντελώς άχρηστο για έναν domain controller, συνεπάγεται και την καλύτερη αξιοποίηση των πόρων του υπολογιστή μας. Αν φοβόσαστε ότι η διαχείριση του Active Directory από την κονσόλα αποτελεί μεγάλο μπελά, πρέπει να σας πούμε ότι δεν σκοπεύουμε να μείνουμε στη γραμμή εντολών. Για την ώρα, όμως, δεν θα αποκαλύψουμε περισσότερα.

Αρχικές ρυθμίσεις

Η εγκατάσταση του Ubuntu Server είναι ιδιαίτερα απλή διαδικασία και δεν θα δυσκολέψει κανέναν αναγνώστη. Το μόνο σημείο που θέλει προσοχή σχετίζεται με τη ρύθμιση της ζώνης ώρας. Τώρα, μπορεί να σκεφτόσαστε ότι τα χάσαμε, αλλά έχετε υπόψη ότι η εύρυθμη λειτουργία του Kerberos απαιτεί από τον server να έχει πάντα τη σωστή ώρα. Ακριβώς γι' αυτό, λίγο αργότερα θα φροντίσουμε για την εγκατάσταση ενός NTP client (περισσότερα για το Network Time Protocol στο άρθρο "Δικτυακές καμπάνες", στο τεύχος 029). Όπως και να 'χει, με ή χωρίς NTP η σωστή ζώνη ώρας είναι απαραίτητη. Όταν ολοκληρωθεί η εγκατάσταση του λειτουργικού, εισερχόμαστε στο σύστημα και πριν απ' οτιδήποτε άλλο φροντίζουμε να πάρουμε όλες τις ενημερώσεις. Κάτι τέτοιο προϋποθέτει τα εξής δύο βήματα: Την ενημέρωση των αποθετηρίων και την ενημέρωση των εγκατεστημένων πακέτων. Για να πετύχουμε και τα δύο με μία κίνηση, αρκεί να εκτελέσουμε κάτι τέτοιο:

```
$ sudo apt-get update && sudo apt-get dist-upgrade
```

Στη συνέχεια προχωράμε στην εγκατάσταση του NTP daemon:

```
$ sudo apt-get install ntp
```

Οι NTP servers που χρησιμοποιούνται εξ ορισμού, αναφέρονται στο αρχείο /etc/ntp.conf:

```
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org
```

Αν θέλετε να προσθέσετε ή να αφαιρέσετε κάποιον time server, μπορείτε να το κάνετε τροποποιώντας κατάλληλα το περιεχόμενο του αρχείου. Εμείς πάντως δεν είχαμε κανένα λόγο να πειράξουμε τη συγκεκριμένη λίστα. Στη συνέχεια, για να επιβάλλουμε την άμεση ενημέρωση της ώρας, εκτελέσαμε διαδοχικά τα εξής:

```
$ sudo service ntp stop
$ sudo ntpdate -B 0.ubuntu.pool.ntp.org
$ sudo service ntp start
```

```
petros@samba:~$ sudo service ntp restart
[sudo] password for petros:
 * Stopping NTP server ntpd                                                [ OK ]
 * Starting NTP server ntpd                                                [ OK ]
petros@samba:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 dbs01.microbase 193.204.114.232  2 u    9   64    1   35.342   -0.656   0.000
 cache.asda.gr   192.53.103.104   2 u    8   64    1   36.604    2.983   0.000
 sucker.mfa.gr   .INIT.          16 u    -   64    0    0.000    0.000   0.000
 ntp2.xe.gr      194.177.210.54   2 u    7   64    1   35.834    0.097   0.000
 golem.canonical .INIT.          16 u    -   64    0    0.000    0.000   0.000
petros@samba:~$
```

Με τον ntp daemon μπορούμε να είμαστε σίγουροι ότι το σύστημα και ολόκληρο το Domain θα έχουν πάντα τη σωστή ώρα.

Σειρά έχει η ρύθμιση της σύνδεσης στο δίκτυο. Ξέρουμε τι σκεφτόσαστε τώρα: Εφόσον λάβαμε ενημερώσεις και πήραμε την ώρα από κάποιον time server, το σύστημα είναι ήδη συνδεδεμένο στο Internet. Τι ακριβώς θα ρυθμίσουμε; Κοιτάξτε, μπορεί να έχουμε πρόσβαση στο Internet και σε κάθε άλλο μηχάνημα του τοπικού δικτύου, αλλά η σύνδεσή μας βασίζεται σε ρυθμίσεις που λάβαμε από τον router, μέσω της υπηρεσίας DHCP. Κάτι τέτοιο δεν συνιστά πρόβλημα για ένα απλό σύστημα, αλλά είναι απαράδεκτο για έναν server. Εφόσον το σύστημα που στήνουμε θα παίζει κομβικό ρόλο στο τοπικό μας δίκτυο, είναι προτιμότερο να έχει σταθερή διεύθυνση IP. Για να αποτρέψουμε τη χρήση του DHCP και να επιβάλλουμε τις δικές μας μόνιμες ρυθμίσεις, πρέπει να επέμβουμε στο αρχείο /etc/network/interfaces. Πριν το ανοίξουμε, μπορούμε να ρίξουμε μια ματιά στις τρέχουσες ρυθμίσεις, ώστε να θυμηθούμε ποια περιοχή διευθύνσεων χρησιμοποιείται στο τοπικό μας δίκτυο, ποια είναι η διεύθυνση του gateway κ.λπ. Κάτι τέτοιο επιτυγχάνεται εκτελώντας το ifconfig:

```
$ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:86:2d:4b
          inet addr:192.168.1.108  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe86:2d4b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10810 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4348 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7635199 (7.2 MiB)  TX bytes:652095 (636.8 KiB)
lo        Link encap:Local Loopback
```

```
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:134128 errors:0 dropped:0 overruns:0 frame:0
            TX packets:134128 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:8050376 (7.6 MiB)  TX bytes:8050376 (7.6 MiB)
```

Στο παραπάνω παράδειγμα, τα στοιχεία που μας ενδιαφέρουν βρίσκονται στην ενότητα eth0. Αφού σημειώσουμε όσα στοιχεία επιθυμούμε, μπορούμε να ανοίξουμε το αρχείο ρυθμίσεων:

```
$ sudo nano /etc/network/interfaces
```

Εκεί, πρέπει να εντοπίσουμε και να διαγράψουμε την ακόλουθη γραμμή:

```
iface eth0 inet dhcp
Στη θέση της προσθέτουμε τα εξής:
iface eth0 inet static
address 192.168.1.5
network 192.168.1.1
netmask 255.255.255.0
broadcast 192.168.1.255
gateway 192.168.1.1
dns-search delta.local
dns-nameservers 192.168.1.5 8.8.8.8
```

Το δικό μας δίκτυο χρησιμοποιεί διευθύνσεις της μορφής 192.168.1.xxx και ειδικά για το σύστημά μας επιλέξαμε την 192.168.1.5. Προσέξτε τώρα τις δύο τελευταίες γραμμές. Με την πρώτη από αυτές καθορίζουμε το domain name που θέλουμε να προσαρτάται αυτόματα στα ονόματα των διαφόρων μηχανημάτων του δικτύου μας. Αυτή η ρύθμιση θα διευκολύνει αργότερα τις μεταφράσεις (resolution) των ονομάτων και την αντιστοίχισή τους σε διευθύνσεις IP. Στη δεύτερη γραμμή προσδιορίζουμε τους name servers που θα χρησιμοποιούνται στο τοπικό μας δίκτυο. Όπως βλέπετε, το όνομα που επιλέξαμε για το δικό μας domain είναι delta, ενώ το TLD (top level domain name) είναι local. Επιπρόσθετα, ως name server θα χρησιμοποιείται το ίδιο το μηχάνημά μας (192.168.1.5), καθώς και ο δημόσιος DNS της Google – αν και αργότερα θα τον απομακρύνουμε.

```
  GNU nano 2.2.6           File: /etc/network/interfaces                Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.5
netmask 255.255.255.0
network 192.168.1.1
broadcast 192.168.1.255
gateway 192.168.1.1
dns-nameservers 192.168.1.5 8.8.8.8
dns-search delta.local

# This is an autoconfigured IPv6 interface
iface eth0 inet6 auto




^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Από το αρχείο /etc/network/interfaces απενεργοποιούμε τη χρήση της υπηρεσίας DHCP και ορίζουμε μια στατική διεύθυνση για τον Domain Controller.

Μετά από την προσθήκη των γραμμών που είδαμε, αποθηκεύουμε το αρχείο /etc/netwotk/interfaces και κλείνουμε τον editor. Σε αυτή τη φάση απομένουν δύο ακόμα απλές ρυθμίσεις. Αφενός πρέπει να καθορίσουμε το δικτυακό όνομα του μηχανήματός μας, αφετέρου πρέπει να αντιστοιχίσουμε στο όνομα τη διεύθυνση που επιλέξαμε προηγουμένως. Αυτές οι ρυθμίσεις πραγματοποιούνται από τα αρχεία /etc/hostname και /etc/hosts αντίστοιχα. Μέσα στο πρώτο βάζουμε το όνομα του μηχανήματος μαζί με το domain name (εμείς επιλέξαμε το samba.delta.local), ενώ μέσα στο δεύτερο αρχείο προσθέτουμε μια γραμμή της ακόλουθης μορφής:

```
<διεύθυνση IP> <πλήρες όνομα μηχανήματος>
```

Στο δικό μας μηχάνημα, η παραπάνω γραμμή είχε ως εξής:

```
192.168.1.5 samba.delta.local
```

Τώρα μπορούμε να προχωρήσουμε σε μια επανεκκίνηση:

```
$ sudo reboot
```

Κύριος εξοπλισμός

Μόλις επανέλθει το σύστημα μπορούμε να κάνουμε μια γρήγορη επιβεβαίωση. Αρκεί να τρέξουμε το προγραμματάκι ifconfig και στη συνέχεια το hostname, ώστε να τσεκάρουμε αν οι ρυθμίσεις εφαρμόστηκαν με επιτυχία. Εφόσον η δικτυακή σύνδεση λειτουργεί κανονικά, προχωράμε στην εγκατάσταση του Kerberos με τη βοήθεια του apt-get:

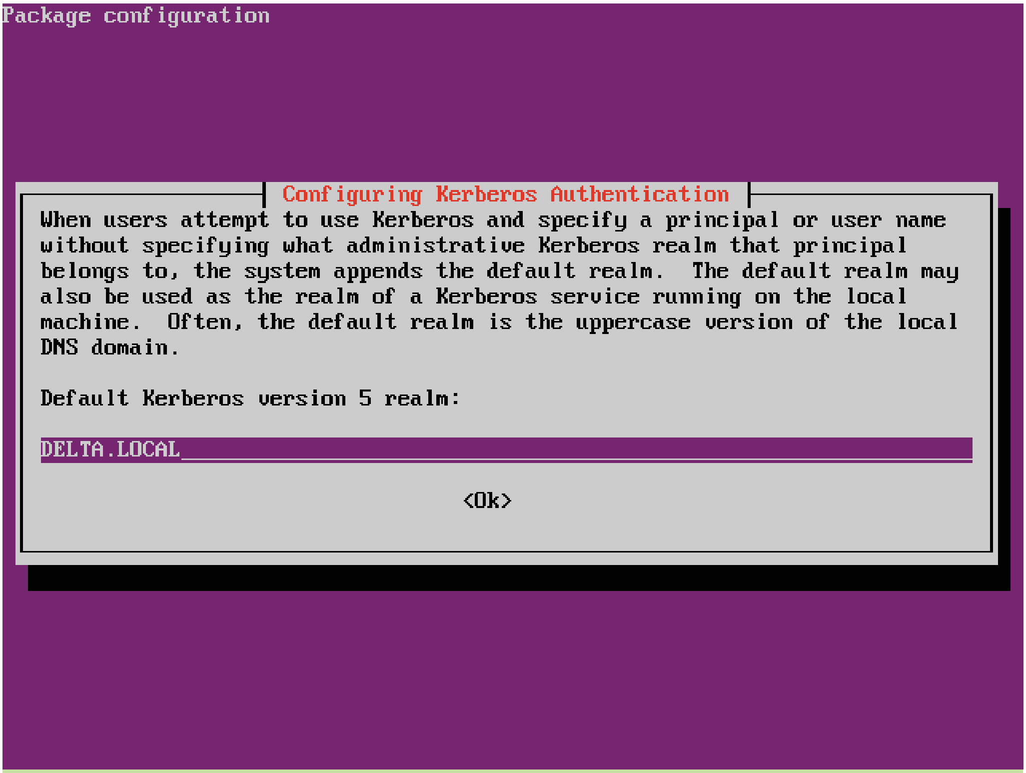
```
$ sudo apt-get install krb5-kdc krb5-user
```

Το πρώτο πακέτο (krb5-kdc) εγκαθιστά τα εξαρτήματα Authentication Service και Key Distribution Center του Kerberos, ενώ το δεύτερο πακέτο (krb5-user) εγκαθιστά ορισμένα βοηθητικά εργαλεία για τη διαχείριση της υπηρεσίας. Έχετε υπόψη ότι το πακέτο krb5 βασίζεται σε μια σωρεία άλλων πακέτων, που το apt-get θα προσπαθήσει να εγκαταστήσει αυτόματα. Στη σχετική ερώτηση για το αν θέλουμε κάτι τέτοιο πρέπει να απαντήσουμε θετικά, χωρίς την παραμικρή ανησυχία για τη διάρκεια της εγκατάστασης ή για το διαθέσιμο χώρο του δίσκου (τα απαιτούμενα πακέτα είναι πολύ μικρά).

```
Reading state information... Done
The following extra packages will be installed:
  attr krb5-config krb5-user libaio1 libavahi-client3 libavahi-common-data
  libavahi-common3 libcups2 libfile-copy-recursive-perl libgmp10
  libgssapi-krb5-2 libgssrpc4 libhdb9-heimdal libkadm5clnt-mit9
  libkadm5srv-mit9 libkdb5-7 libkdc2-heimdal libkrb5-3 libkrb5support0 libldb1
  libntdb1 libopts25 libtalloc2 libtdb1 libtevent0 libverto-libevent1
  libverto1 libwbclient0 python-crypto python-dnspython python-ldb python-ntdb
  python-samba python-talloc python-tdb samba-common samba-common-bin
  samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools update-inetd
Suggested packages:
  openbsd-inetd inet-superserver krb5-kdc-ldap cups-common krb5-doc ntp-doc
  python-crypto-dbg python-crypto-doc bind9 bind9utils ldb-tools smbldap-tools
  winbind heimdal-clients
The following NEW packages will be installed:
  attr krb5-admin-server krb5-config krb5-kdc krb5-user libaio1
  libavahi-client3 libavahi-common-data libavahi-common3 libcups2
  libfile-copy-recursive-perl libgmp10 libgssrpc4 libhdb9-heimdal
  libkadm5clnt-mit9 libkadm5srv-mit9 libkdb5-7 libkdc2-heimdal libldb1
  libntdb1 libopts25 libtalloc2 libtdb1 libtevent0 libverto-libevent1
  libverto1 libwbclient0 ntp python-crypto python-dnspython python-ldb
  python-ntdb python-samba python-talloc python-tdb samba samba-common
  samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
  update-inetd
The following packages will be upgraded:
  libgssapi-krb5-2 libkrb5-3 libkrb5support0
3 upgraded, 43 newly installed, 0 to remove and 39 not upgraded.
Need to get 9,629 kB of archives.
After this operation, 50.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Τα πρόσθετα πακέτα που απαιτούνται για την εγκατάσταση των Kerberos και Samba είναι αρκετά. Μην σας τρομάζει το πλήθος τους: Πρόκειται για μικρά προγράμματα που θα κατέβουν αμέσως και θα καταλάβουν ελάχιστο χώρο στο δίσκο.

Όταν ολοκληρωθεί η εγκατάσταση, θα εκτελεστεί αυτόματα το Kerberos Authentication Configuration Tool. Το συγκεκριμένο εργαλείο ζητά από το χρήστη ορισμένα δεδομένα για τη βασική ρύθμιση του Kerberos.



Μετά την εγκατάσταση του Kerberos θα χρειαστεί να πραγματοποιήσουμε μια πρώτη, βασική ρύθμιση της υπηρεσίας. Αργότερα θα αλλάξουμε όλες τις ρυθμίσεις με τη βοήθεια του samba-tool, αλλά είναι φρόνιμο να μην προσπεράσουμε αυτό το βήμα και να φανούμε προσεκτικοί.

Στο πεδίο default realm βάζουμε το domain name που επιλέξαμε για το τοπικό μας δίκτυο, ενώ στο πεδίο Administrative Server δίνουμε το hostname του μηχανήματος. Σημειώστε ότι και στις δύο περιπτώσεις πρέπει να πληκτρολογήσουμε τα ονόματα με κεφαλαίους χαρακτήρες! Εμείς, για παράδειγμα, ως default realm δώσαμε το DELTA.LOCAL, ενώ ως Administrative Server δώσαμε το Samba.DELTA.LOCAL. Αμέσως μετά προχωράμε στην εγκατάσταση της Samba:

```
$ sudo apt-get install samba smbclient
```

Όπως καταλαβαίνετε, το πακέτο samba εγκαθιστά τον Samba server, ενώ το πακέτο smbclient περιλαμβάνει εργαλεία για τη σύνδεση στον πρώτο. Με τα βοηθητικά εργαλεία θα πραγματοποιήσουμε τις πρώτες δοκιμές μας. Όπως και στην περίπτωση του Kerberos, η εγκατάσταση του samba συμπαρασύρει πολλά άλλα πακέτα. Στη

σχετική ερώτηση του apt-get πρέπει να απαντήσουμε θετικά, αλλά και πάλι χωρίς ανησυχία. Σκεφτείτε ότι όλα τα απαιτούμενα πακέτα για τη λειτουργία των Kerberos και Samba, καταλαμβάνουν σχεδόν 50MB. Μιλάμε για ψίχουλα! Μήπως αναρωτιέστε τι μας έπιασε κι επιμένουμε τόσο πολύ στον αποθηκευτικό χώρο; Με τη λύση που παρουσιάζουμε, ο πανάκριβος και βαρύς Windows Server θα μπορούσε να αντικατασταθεί από ένα παλιό και παραμελημένο μηχάνημα – ή ακόμα και από ένα λιλιπούτειο Raspberry Pi.

Μόλις ολοκληρωθεί κι αυτός ο κύκλος εγκαταστάσεων, μπορούμε να ξεκινήσουμε τον Samba server και, ουσιαστικά, να ενεργοποιήσουμε τον Domain Controller. Για το σκοπό αυτό θα χρησιμοποιήσουμε το εργαλείο samba-tool. Πριν το τρέξουμε όμως πρέπει να μετονομάσουμε το αρχείο με τις υπάρχουσες ρυθμίσεις του Samba server. Με αυτόν τον τρόπο αποφεύγουμε την ενδεχόμενη εμφάνιση ορισμένων σφαλμάτων.

```
$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.old
```

Ουσιαστικά, με την παραπάνω μετονομασία εξασφαλίζουμε την απομάκρυνση όλων των εργοστασιακών ρυθμίσεων. Στη συνέχεια μπορούμε να ξεκινήσουμε το samba-tool ως εξής:

```
$ sudo samba-tool domain provision --use-rfc2307 --interactive --use-ntvfs
```

Το εργαλείο θα ξεκινήσει και θα μας απευθύνει μια σειρά ερωτήσεων για τη λειτουργία του domain controller που θέλουμε να στήσουμε. Οι προεπιλεγμένες απαντήσεις είναι ικανοποιητικές και στα περισσότερα βήματα μπορούμε να δίνουμε ένα ENTER. Κατά τη διάρκεια των δικών μας δοκιμών, δώσαμε τα ακόλουθα στοιχεία:

```
Realm: DELTA.LOCAL
Domain: DELTA
Server Role: dc
DNS Backend: SAMBA_INTERNAL
DNS Forwarder IP: 8.8.8.8
Administrator Password: sTronGPaSsw0rd
```

Προφανώς, στα πεδία Realm και Domain δίνουμε τα αντίστοιχα ονόματα που επιλέξαμε για το τοπικό μας δίκτυο, ενώ στο DNS Forwarder μπορούμε να χρησιμοποιήσουμε οποιονδήποτε άλλο DNS server και όχι κατ' ανάγκη αυτόν της Google (8.8.8.8). Ο κωδικός διαχειριστή που δίνουμε εδώ, απαιτείται για την προσθήκη κάθε νέου συστήματος στο domain. Έχετε υπόψη ότι το μήκος του πρέπει να ξεπερνά τους 8 χαρακτήρες και να περιλαμβάνει πεζά, κεφαλαία και αριθμούς. Σημειώστε επίσης ότι για λόγους ασφάλειας, ο κωδικός του διαχειριστή έχει και ημερομηνία λήξης. Αν το δικό σας τοπικό δίκτυο χρησιμοποιείται από χρήστες που εμπιστεύεστε και

θεωρείτε υπερβολικά τα μέτρα ασφαλείας περί του κωδικού, δεν υπάρχει λόγος να δυσαnασχετείτε. Με τη βοήθεια του samba-tool μπορούμε να αλλάξουμε τις σχετικές ρυθμίσεις πανεύκολα. Για να επιτρέψουμε τη χρήση απλούστερων κωδικών, αρκεί να δώσουμε κάτι τέτοιο:

```
$ sudo samba-tool domain passwordsettings set --complexity=off
```

Όσο για τη λειτουργία λήξης του κωδικού, μπορούμε να την απενεργοποιήσουμε ως εξής:

```
$ sudo samba-tool user setexpiry Administrator --noexpiry
```

Τέλος, στην περίπτωση που ξεχάσουμε τον κωδικό, μπορούμε να τον αλλάξουμε γράφοντας κάτι τέτοιο:

```
$ sudo samba-tool user setpassword Administrator
```

Πάντως, ανεξάρτητα από τη φύση του δικού σας δικτύου και την εμπιστοσύνη που νιώθετε προς τους χρήστες, εμείς θα σας προτείναμε να μην καταργήσετε κανένα από τα δύο μέτρα ασφαλείας. Θα ήταν φρόνιμο να μην απλοποιήσετε τη μορφή του κωδικού και να απενεργοποιήσετε μόνο την αυτόματη λήξη. Χρησιμοποιώντας "ευκολότερους" κωδικούς υποβαθμίζετε σε μεγάλο βαθμό την ασφάλεια του domain και δεν υπάρχει κανένας λόγος να κάνετε κάτι τέτοιο.

Αν δεν το έχετε αντιληφθεί ακόμα, πρέπει να σας πούμε ότι το samba-tool είναι εξαιρετικό εργαλείο. Σκεφθείτε ότι ρυθμίζοντας το Samba server, το προγραμματάκι ετοιμάζει αυτομάτως κι ένα αρχείο ρυθμίσεων για το Kerberos. Εμείς, για λόγους ασφάλειας (φύλαγε τα ρούχα σου), δεν διαγράψαμε το παλιό αρχείο ρυθμίσεων του Kerberos, αλλά φροντίσαμε να το μετονομάσουμε:

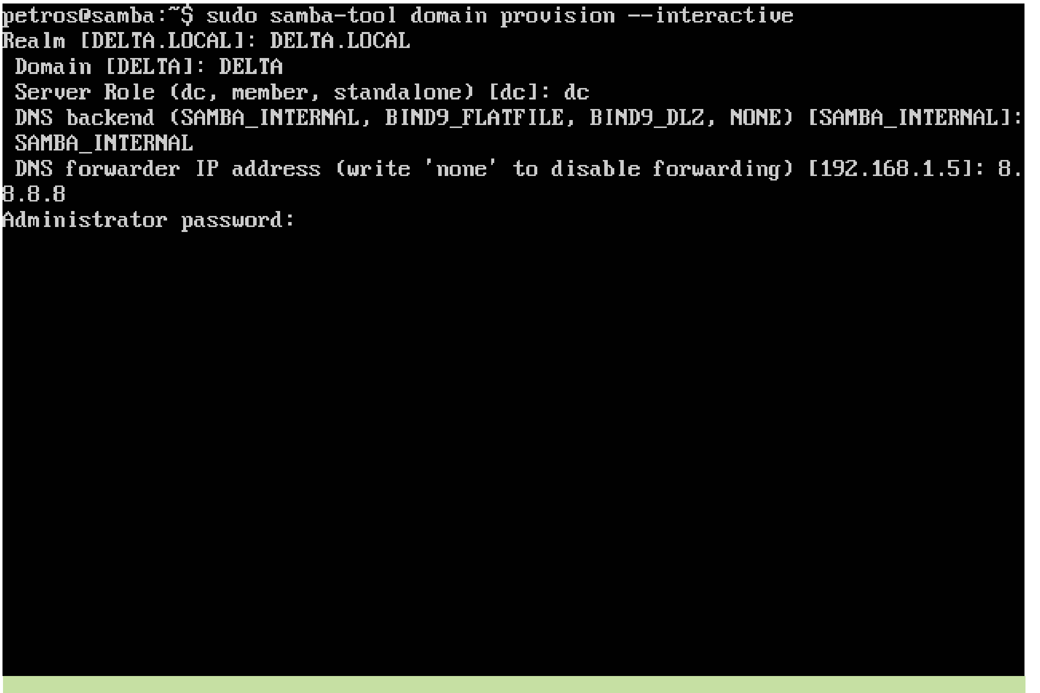
```
$ sudo mv /etc/krb5.conf /etc/krb5.conf.old
```

Αν νομίζετε ότι συνεχίσαμε μετακινώντας το αρχείο που δημιούργησε το samba-tool, κάνετε λάθος. Το συγκεκριμένο εργαλείο ενδέχεται να το χρησιμοποιήσουμε αρκετές φορές ακόμα και κάθε φορά θα παράγει ένα νέο αρχείο ρυθμίσεων για το Kerberos. Για να μην χρειάζεται κάθε φορά η κατάλληλη μετακίνηση/αντιγραφή, κάναμε κάτι πιο πονηρό: Δημιουργήσαμε ένα σύνδεσμο (soft link) από τη θέση όπου το samba-tool παράγει το αρχείο ρυθμίσεων, προς τη θέση όπου περιμένει να τις βρει το Kerberos:

```
$ sudo ln -sf /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Με αυτό το κολπάκι, η ρύθμιση του Kerberos δεν θα μας απασχολήσει ποτέ ξανά. Θα χρησιμοποιούμε μόνο το samba-tool και όλα τα υπόλοιπα θα γίνονται αυτόματα.

Μέσα στον όλο ενθουσιασμό που μας διακατέχει, ξεχάσαμε να σας πούμε κάτι σημαντικό: Ο Domain Controller είναι έτοιμος να σερβίρει τις υπηρεσίες του Active Directory σε όλους τους υπολογιστές του τοπικού δικτύου που τρέχουν Windows! Αν θέλετε να μάθετε πώς θα τις αξιοποιήσετε, πηγαίνετε τώρα στο άρθρο που αρχίζει από τη σελίδα 60 του τεύχους.



Το samba-tool αποτελεί ένα πολυεργαλείο και μάλιστα πολύτιμο. Με τη βοήθειά του μπορούμε πανεύκολα να αναθέσουμε στον Samba server το ρόλο του Domain Controller.

Skill: Intermediate
Tags: Seedbox, BitTorrent, Transmission, TorGuard, OpenVPN, DNS leaks, iptables

Στον αγώνα για ανέμελο torrenting, μέρος 2/3

Δημιουργία βολικού κι ασφαλούς Seedbox

Φανταζόμαστε πως θα συμφωνείτε κι εσείς ότι αλλιώς ακούγεται όταν μιλάμε για "κατεβαστήρι" κι αλλιώς όταν μιλάμε για "Seedbox". Όπως και να 'χει, το προαναφερθέν είναι ένα κατεβαστήρι όπου χρησιμοποιείται το πρωτόκολλο BitTorrent. Θα δούμε σε λίγο ότι είναι πολύ βολικό να έχουμε το δικό μας Seedbox. Φυσικά, πέρα από την ευκολία χρειαζόμαστε κι ασφάλεια – ή ακριβέστερα ανωνυμία *και* ιδιωτικότητα. Ευτυχώς, μπορούμε να τα έχουμε και τα δύο.

του Χρήστου Βαρελά

Το Seedbox που πρόκειται να φτιάξουμε θα κατοικεί στο οικιακό μας δίκτυο κι όχι στο cloud. Αυτό θα φανεί παράξενο στους επαγγελματίες downloaders, αφού τα Seedbox στο cloud παρέχουν τρομακτικές ταχύτητες download/upload αλλά κι ανωνυμία για τους χρήστες τους. Πράγματι, έτσι έχουν τα πράγματα, μόνο που εμείς δεν είμαστε επαγγελματίες downloaders. Τι να κάνουμε, δεν συνηθίζουμε να κατεβάζουμε το τοπικό χωροχρονικό συνεχές, οπότε οι υψηλές ταχύτητες download/upload δεν μας ελκύουν ιδιαίτερα. Όταν μάλιστα συνυπολογίζουμε το σχετικά υψηλό κόστος ενός καλού Seedbox και στο καπάκι θυμόμαστε ότι χρειάζεται να συμμετέχουμε σε κάποιον private tracker, τότε σηκώνουμε τους ώμους αδιάφορα, γυρίζουμε το κεφάλι *ελαφρώς* στο πλάι και βγάζουμε μια απαξιωτική φωνούλα του στιλ "μ(ι) εεε" (ένρινα και το "ι" μόλις που ακούγεται). Τότε, λοιπόν, τι στο καλό το θέλουμε το Seedbox, μέσα στο τοπικό μας δίκτυο;

Πολύ απλά, για το περιστασιακό downloading μέσω BitTorrent προτιμάμε ένα Linux box –εικονικό ή φυσικό δεν έχει σημασία–, χωρίς οθόνη. Η διαχείριση του box γίνεται από τη γραμμή εντολών, με απομακρυσμένη σύνδεση μέσω SSH. Ο δε χειρισμός των torrents και του downloading γίνεται επίσης από τη γραμμή εντολών, π.χ., με τη βοήθεια ενός εργαλείου σαν το rtorrent ή σαν το transmission-cli. Επιπρόσθετα, παρέχεται κι ένα κατάλληλο web panel ώστε να εργαζόμαστε από άλλον υπολογιστή κι από τον browser της προτίμησής μας. Για τα ζητήματα της ανωνυμίας και της

ιδιωτικότητας καταφεύγουμε στη λύση του TorGuard, ώστε αφενός ο ISP μας να μην έχει ιδέα για το τι κάνουμε (privacy), αφετέρου να μηδενιστεί η πιθανότητα λήψης προειδοποιητικών emails του στιλ "σταματήστε το downloading ή υποστείτε τις συνέπειες" (anonymity, βλ. και άρθρο στη σελίδα 14).

Οι προδιαγραφές του Seedbox

Αν έχετε Raspberry Pi model B ή καλύτερο και σκεφτόσαστε πώς να το αξιοποιήσετε, να ξέρετε ότι δύναται ν' αποτελέσει άριστο Seedbox. Κατά πάσα πιθανότητα θα του συνδέσετε κι έναν εξωτερικό δίσκο USB, αλλά σε κάθε περίπτωση μιλάμε για ένα κομψό, αθόρυβο κι ενεργειακά οικονομικό setup. Αυτή την περίοδο δεν μας περισσεύει κάποιο Raspberry Pi, οπότε αποφασίσαμε να δημιουργήσουμε ένα νέο KVM VM στον virtualization host με το openSUSE που έχουμε (https://deltahacker.gr/?p=15388). Στην εικονική μηχανή δώσαμε 768MiB RAM, δύο επεξεργαστές και δυναμικό σκληρό δίσκο 64GiB. Ως guest OS επιλέξαμε το Ubuntu Server 14.04 LTS 64bit και μετά την εγκατάστασή του φροντίσαμε και προσαρτήσαμε ένα exported NFS directory, από τον virtualization host. (Για το NFS και την προσάρτηση exported directories διαβάστε στο https://deltahacker.gr/?p=15549.) Σ' αυτή τη θέση αποθηκεύονται τα αρχεία που κατεβαίνουν. Είναι μάλιστα εύκολη η μεταφορά τους σε άλλο exported NSF directory, το οποίο βλέπει ένα KVM VM σε ρόλο Plex media server. Αλλά ας μην ξεφεύγουμε. Πριν συνεχίσουμε, ας σημειώσουμε πως δεν είναι απαραίτητο να δουλέψετε κι εσείς σε εικονικό περιβάλλον. Ίσως, π.χ., αποφασίσετε να δώσετε νέα αποστολή σε ένα ταπεινό PC που μέχρι σήμερα δεν σας εξυπηρετούσε.

Προετοιμασία του OS

Κατά την εγκατάσταση του Ubuntu ζητήσαμε να εγκατασταθεί και να ενεργοποιηθεί ο OpenSSH server. Να σημειώσουμε εδώ ότι στα Linux VMs/boxes που έχουμε, φροντίζουμε ώστε να συνδεόμαστε όχι με πληκτρολόγηση username/password αλλά με βάση το κατάλληλο ζεύγος ιδιωτικού/δημοσίου κλειδιού. Περισσότερα επ' αυτού διαβάστε στο https://deltahacker.gr/?p=13357.

Όταν ολοκληρώθηκε η εγκατάσταση του λειτουργικού συνδεθήκαμε στο VM απομακρυσμένα, μέσω SSH, κι αμέσως ενημερώσαμε την τοπική λίστα με τα διαθέσιμα πακέτα των αποθετηρίων (repositories):

```
sub0@seedbox:~$ sudo apt-get update
```

Στη συνέχεια αναβαθμίσαμε τα όποια πακέτα χρειάζονταν αναβάθμιση:

```
sub0@seedbox:~$ sudo apt-get dist-upgrade
```

Όπως βλέπετε, οι εργασίες που απαιτούν δικαιώματα διαχειριστή (root) γίνονται από το λογαριασμό του απλού μας χρήστη (sub0) και με τη βοήθεια του sudo. Την πρώτη φορά που καλούμε το sudo μάς ζητείται η πληκτρολόγηση password. Σημει-

ώστε ότι αυτό δεν ζητείται διαρκώς. Ακριβέστερα, το sudo ζητά password μόνον εφόσον έχουν περάσει τουλάχιστον 15 λεπτά από την τελευταία φορά που το δώσαμε. Το θέμα είναι ότι στο συγκεκριμένο VM δεν υπάρχει λόγος να πληκτρολογούμε password για το sudo, ούτε μία φορά. Προκειμένου λοιπόν να μη μας ζητηθεί ξανά password για το sudo, πληκτρολογούμε

```
sub0@seedbox:~$ sudo visudo
```

και στο τέλος του αρχείου που ανοίγει προσθέτουμε την ακόλουθη γραμμή:

```
sub0 ALL=(ALL) NOPASSWD: ALL
```

Στο Ubuntu, ο editor που καλείται με το visudo δεν είναι το vi αλλά το nano. Έτσι, για ν' αποθηκεύσουμε την αλλαγή πατάμε το συνδυασμό πλήκτρων [CTRL+O] και μετά το [Enter]. Τον editor τον εγκαταλείπουμε δίνοντας [CTRL+X]. Η αλλαγή θα ληφθεί υπόψη την επόμενη φορά που θα συνδεθούμε στο λογαριασμό μας, οπότε κάνουμε τώρα ένα logout κι αμέσως μετά ένα (SSH) login.

Τώρα, αν στο τερματικό σας βλέπετε ειδοποιήσεις περί locales που δεν έχουν οριστεί κ.λπ., τότε με δικαιώματα διαχειριστή ανοίξτε το αρχείο /etc/default/locale...

```
sub0@seedbox:~$ sudo nano /etc/default/locale
```

...και φροντίστε ώστε τα περιεχόμενά του να μοιάζουν με τα ακόλουθα:

```
LANG="en_US.UTF-8"
LC_ALL="en_US.UTF-8"
LANGUAGE="en_US.UTF-8"
```

Αποθηκεύστε την αλλαγή, εγκαταλείψτε τον editor και μετά πληκτρολογήστε

```
sub0@seedbox:~$ sudo locale-gen
```

Εγκατάσταση Transmission

O BitTorrent client που επιλέγουμε για το Seedbox μας είναι το άριστο Transmission, το οποίο μεταξύ άλλων παρέχει κι ένα απλό, όμορφο και λειτουργικό web panel. Από οποιονδήποτε υπολογιστή του τοπικού δικτύου και με τον web browser της προτίμησής μας, θα συνδεόμαστε στο εν λόγω panel ώστε ν' ανεβάζουμε torrents για ...κατέβασμα, βεβαίως και για να διαχειριζόμαστε τα downloads. Η εγκατάσταση του Transmission απαιτεί την προσθήκη του κατάλληλου PPA:

```
sub0@seedbox:~$ sudo add-apt-repository ppa:transmissionbt/ppa
```

Αμέσως μετά φρεσκάρουμε όλα τα αποθετήρια...

```
sub0@seedbox:~$ sudo apt-get update
```

...κι εγκαθιστούμε το Transmission ως ακολούθως:

```
sub0@seedbox:~$ sudo apt-get install transmission-cli transmission-common
transmission-daemon
```

Απαραίτητες ρυθμίσεις

Πριν αρχίσουμε να παίζουμε με το Transmission επιβάλλεται να τροποποιήσουμε συγκεκριμένες παραμέτρους της λειτουργίας του. Επειδή ο συγκεκριμένος BitTorrent client λειτουργεί ως υπηρεσία, προς το παρόν τη σταματάμε:

```
sub0@seedbox:~$ sudo service transmission-daemon stop
```

Το κεντρικό αρχείο ρυθμίσεων είναι το /etc/transmission-daemon/settings.json. Το ανοίγουμε με το nano – εννοείται με δικαιώματα διαχειριστή:

```
sub0@seedbox:~$ sudo nano /etc/transmission-daemon/settings.json
```

Εντοπίζουμε τις γραμμές που μοιάζουν με τις ακόλουθες και τις αλλάζουμε για τη δική μας εγκατάσταση (η αρίθμηση δεν υπάρχει στο αρχείο, απλά την προσθέσαμε εμείς εδώ για ευκολία στην αναφορά):

```
1 | "download-dir": "/home/sub0/exported/Downloads",
2 | "incomplete-dir": "/home/sub0/exported/Downloads",
3 | "incomplete-dir-enabled": false,
4 | "rpc-password": " {01965c7d11ff87bbb442f6d1fc1e957bcf316e578JLabmY/"
5 | "rpc-username": "transmission"
6 | "rpc-whitelist": "127.0.0.1,10.20.30.*,192.168.10.*"
```

Ας δούμε λίγο τι γίνεται σε κάθε μία από τις προηγούμενες γραμμές. Στις 1 και 2 ορίζουμε τις πλήρεις διαδρομές των καταλόγων για τα αρχεία που έχουν κατέβει, καθώς και για εκείνα που κατεβαίνουν αλλά το downloading δεν έχει ολοκληρωθεί.

Όπως βλέπετε, προτιμάμε τον ίδιο κατάλογο τόσο για τα ολοκληρωμένα downloads, όσο και για εκείνα εν εξελίξει. Εξ ορισμού πάντως ο φάκελος για τα μη-ολοκληρωμένα downloads δεν χρησιμοποιείται (βλ. γραμμή 3) και προς το παρόν μάς αρέσει αυτό. Αν θέλετε τον εν λόγω κατάλογο, στη γραμμή 3 μην ξεχάσετε ν' αλλάξετε το false σε true. Στις γραμμές 4 και 5 ορίζουμε το όνομα του χρήστη για τη σύνδεση στο web panel, καθώς και το password του. Σημειώστε ότι μόλις ενεργοποιήσουμε ξανά τον Transmission daemon, στο αρχείο settings.json το password θα αντικατασταθεί με το SHA1 hash του. Αυτό που βλέπετε στο παράδειγμά μας, λοιπόν, δεν είναι το password μας αλλά το hash του password. Στη δε γραμμή 6 ορίζουμε από πού επιτρέπονται συνδέσεις στο web panel του Transmission. Λογικό είναι να επιτρέπουμε εκείνες που ξεκινούν από τον ίδιο τον υπολογιστή (127.0.0.1), καθώς κι εκείνες από άλλα μηχανήματα του τοπικού δικτύου. Στο τοπικό μας δίκτυο οι συσκευές έχουν διευθύνσεις IP της μορφής 192.168.10.*. Στο δικό σας μάλλον θα έχουν διευθύνσεις διαφορετικής μορφής, οπότε τροποποιήστε την παράμετρο rpc-whitelist αναλόγως. Θα παρατηρήσατε εξάλλου ότι στην παράμετρο rpc-whitelist έχουμε συμπεριλάβει και διευθύνσεις της μορφής 10.20.30.*. Αυτό το κάναμε διότι τέτοιες διευθύνσεις λαμβάνουν οι clients του OpenVPN server που τρέχει στο pfSense box του τοπικού μας δικτύου (https://deltahacker.gr/?p=12109). Όποτε βρισκόμαστε εκτός τοπικού δικτύου και θέλουμε να ελέγξουμε πώς προχωράει ένα torrent που είχαμε αφήσει να κατεβαίνει, συνδεόμαστε *πρώτα* στον OpenVPN server του pfSense και μετά, από έναν οποιονδήποτε web browser, απλά επισκεπτόμαστε το web panel του Transmission.

Αποθηκεύουμε τις αλλαγές, εγκαταλείπουμε τον editor και στη συνέχεια ανοίγουμε το αρχείο /etc/init/transmission-daemon.conf με το nano – εννοείται με δικαιώματα διαχειριστή:

```
sub0@seedbox:~$ sudo nano /etc/init/transmission-daemon.conf
```

Για την ευκολότερη διαχείριση των αρχείων που κατεβάζουμε, βολεύει ν' αλλάξουμε το λογαριασμό κάτω από τον οποίο τρέχει ο Transmission daemon (στο Ubuntu ονομάζεται debian-transmission) σ' εκείνον του χρήστη μας (sub0). Προς τούτο αρκεί να τροποποιήσουμε κατάλληλα τις τιμές των παραμέτρων setuid και setgid, στο πάνω μέρος του transmission-daemon.conf. Οι αλλαγμένες παράμετροι για τη δική μας εγκατάσταση έχουν ως ακολούθως:

```
setuid sub0
setgid users
```

Εσείς βέβαια στη θέση του sub0 θα βάλετε το username του δικού σας χρήστη, ενώ για το setgid πιθανότατα θα βάλετε το όνομα του group με όνομα ίδιο μ' εκείνο του χρήστη σας. Αν, δηλαδή, το username του χρήστης σας είναι lmtgm (lean, mean, torrent-grabbing machine – λέμε τώρα), τότε στο transmission-daemon.conf θα θέλετε τις ακόλουθες γραμμές:

```
setuid lmtgm
setgid lmtgm
```

(Το ότι εμείς βάλαμε "setgid users" κι όχι " setgid sub0", έχει να κάνει με την ευθυγράμμιση των groups μεταξύ του KVM VM με Ubuntu και του physical host με openSUSE, από το οποίο μέσω NFS μοιράζεται ένας κατάλογος εντός του οποίου αποθηκεύει το Transmission. Δεν είναι κάτι που πρέπει να σας απασχολεί, απλά το αναφέρουμε.) Για άλλη μια φορά αποθηκεύουμε τις αλλαγές κι εγκαταλείπουμε τον editor.

Πριν ξεκινήσουμε τον Transmission daemon, από τη στιγμή που αλλάξαμε το λογαριασμό κάτω από τον οποίο τρέχει οφείλουμε τώρα να αλλάξουμε και το ιδιοκτησιακό καθεστώς των καταλόγων /etc/transmission-daemon, /var/lib/transmission-daemon/info καθώς κι όλων των περιεχομένων τους. Αν δεν το κάνουμε, το Transmission απλά δεν θα ξεκινήσει:

```
sub0@seedbox:~$ sudo chown -R sub0:users /etc/transmission-daemon
sub0@seedbox:~$ sudo chown -R sub0:users /var/lib/transmission-daemon/info
```

Περιττό να σημειώσουμε ότι θα δώσετε τα ονόματα χρήστη και group που ισχύουν για τη δική σας εγκατάσταση. Η ενεργοποίηση του Transmission daemon επιτυγχάνεται πληκτρολογώντας

```
sub0@seedbox:~$ sudo service transmission-daemon start
```

Ένας τρόπος προκειμένου να βεβαιωθούμε ότι τρέχει, είναι να γράψουμε

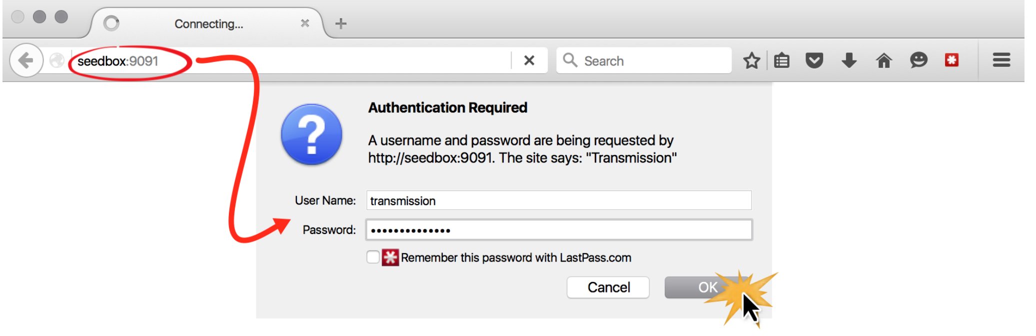
```
sub0@seedbox:~$ sudo netstat -4antp
```

Αν όλα έχουν πάει καλά, στην έξοδο του netstat θα υπάρχει μία γραμμή που υποδηλώνει ότι το Transmission αφουγκράζεται για αιτήσεις πελατών από το port 9091/TCP.

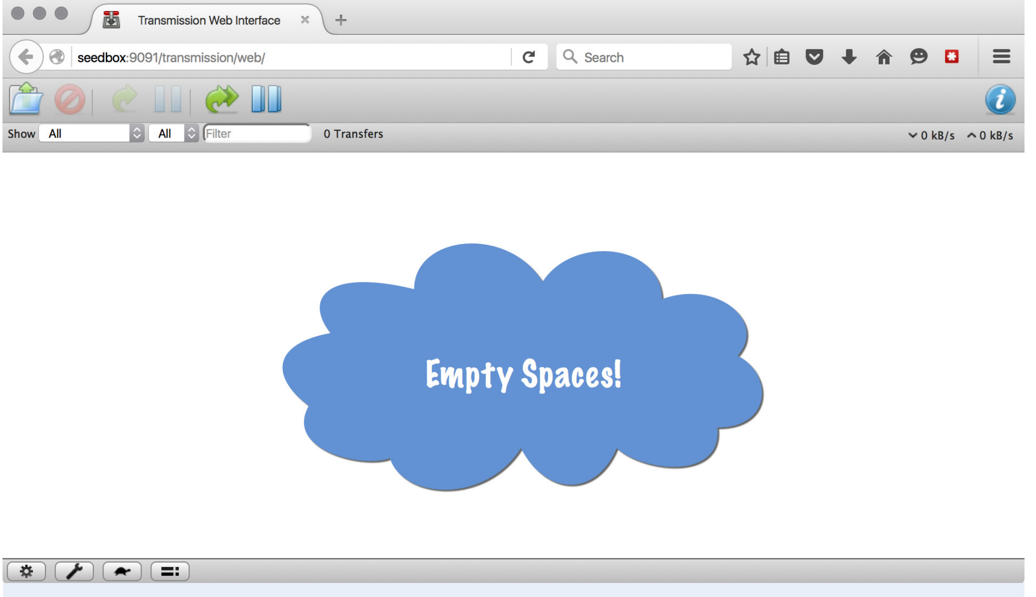
Χρήση του Transmission

Από έναν οποιονδήποτε υπολογιστή του τοπικού μας δικτύου κι από έναν οποιονδήποτε browser, στο web panel του Transmission φτάνουμε με επίσκεψη σε διεύθυνση της μορφής http://IP_address:9091, όπου IP_address είναι η εσωτερική διεύθυνση IP του VM/box σε ρόλο Seedbox. Με κλικ στο σχετικό εικονίδιο ανεβάζουμε ένα ή περισσότερα torrents και μπορούμε, φυσικά, να παρακολουθούμε την πρόοδο ενεργών downloads, να ξεκινάμε νέα, να παγώνουμε και να συνεχίζουμε άλλα κ.ο.κ. Γενικά, το web panel του Transmission είναι απλό αλλά δεν τσιγκουνεύεται τις πληροφορίες που δίνει, ούτε περιορίζει τον χρήστη του.

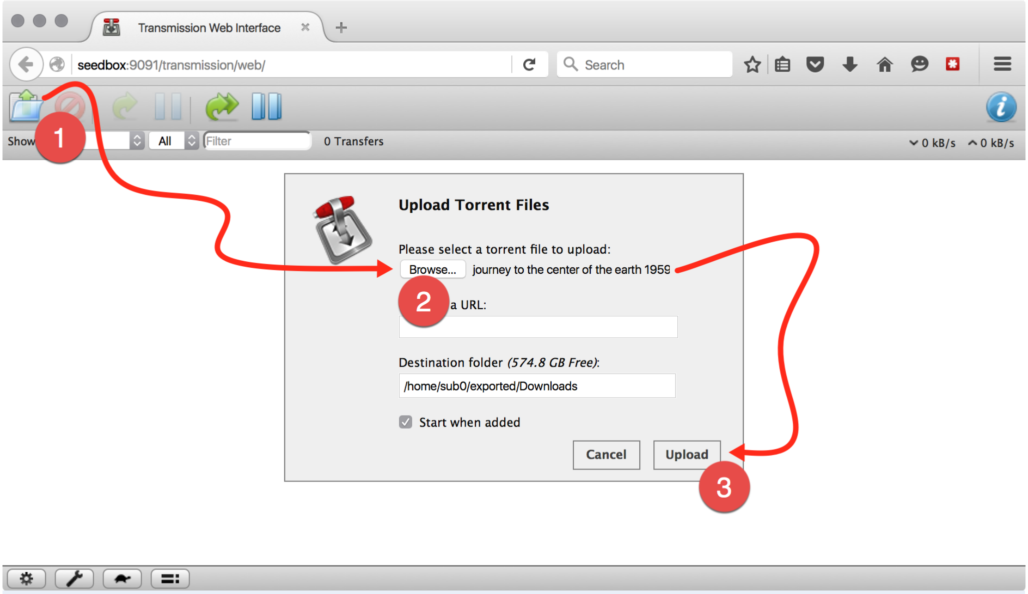
Ένας τρόπος για να λαμβάνουμε τα αρχεία ή τους φακέλους που έχουν ήδη κατέβει στο Seedbox μας, είναι μέσω του πρωτοκόλλου SFTP (FTP over SSH). Το FileZilla (https://filezilla-project.org) είναι ένας δωρεάν FTP client για Linux, OS X και Windows. Αποτελεί Ελεύθερο Λογισμικό και υποστηρίζει, μεταξύ άλλων, συνδέσεις SFTP. Υπάρχουν βέβαια πολλές εναλλακτικές λύσεις και μέθοδοι για τη λήψη ή/και για τη διαχείριση των αρχείων του Seedbox μας, όμως στο παρόν άρθρο άλλα μας απασχολούν.



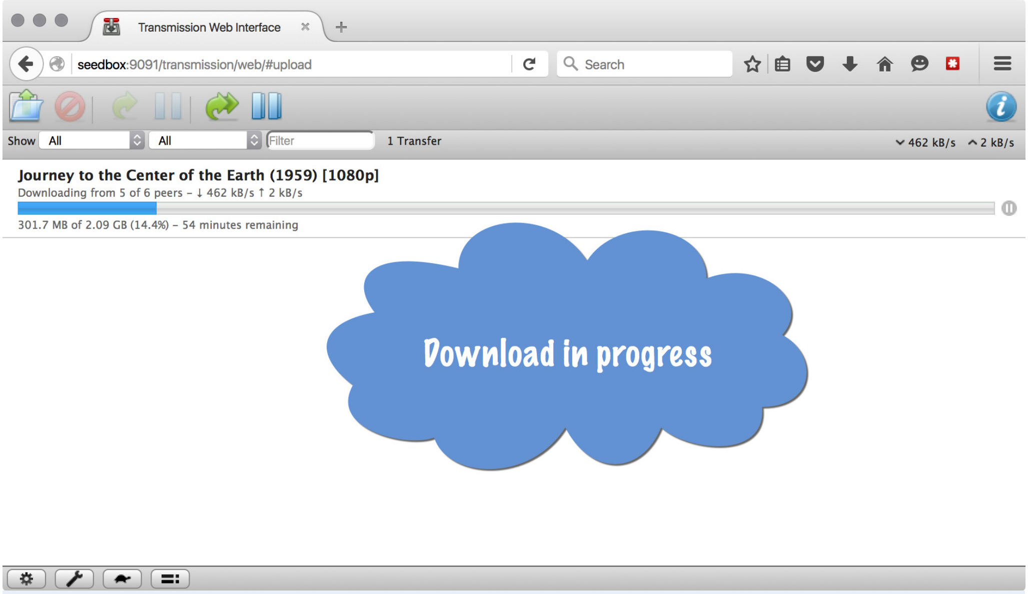
Για τη σύνδεση στο web panel του Transmission αρκεί να επισκεφτούμε μια διεύθυνση της μορφής http://IP_address:9091, όπου το IP_address είναι η εσωτερική διεύθυνση IP που έχει πάρει το Seedbox από τον router. Στο παράδειγμα, αντί για τη διεύθυνση έχουμε απλά πληκτρολογήσει "seedbox" – κι αυτό χάρη στον name server του router μας. Την πρώτη φορά εξάλλου που συνδεόμαστε στο web panel του Transmission, μας ζητούνται username και password.



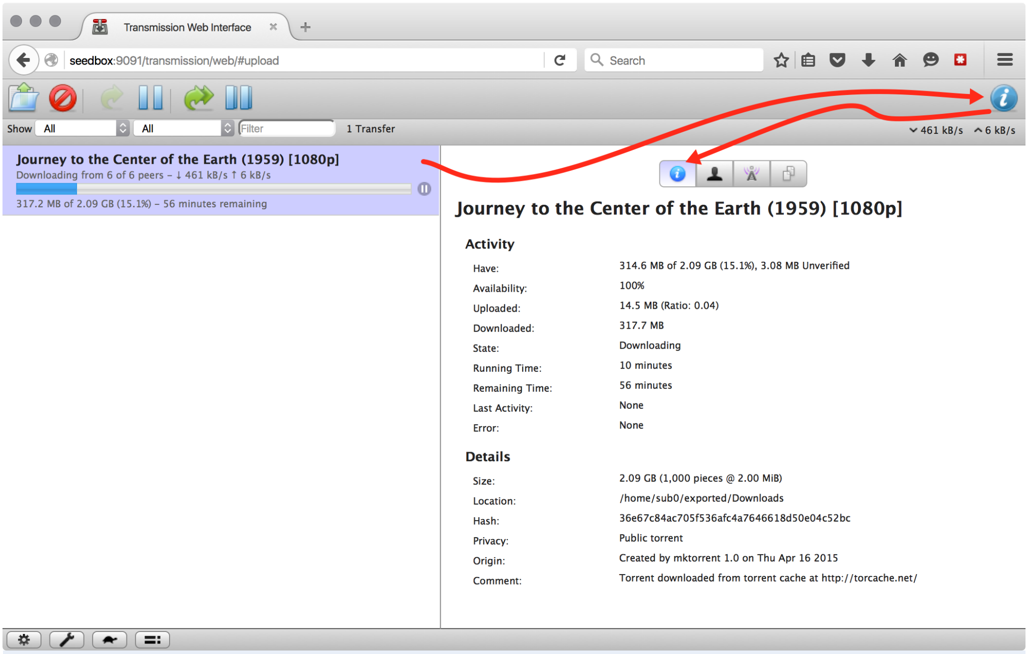
Σε μια πρώτη ματιά, το web panel του Transmission ίσως δείχνει ανησυχητικά άδειο. Είναι πράγματι λιτό, όπως όμως θα διαπιστώσετε την κάνει τη δουλειά του – και μάλιστα με το παραπάνω.



Με κλικ στο σχετικό εικονίδιο (1) εμφανίζεται ένα παραθυράκι επιλογής αρχείων (2), από το οποίο επιλέγουμε ένα torrent από τον τοπικό δίσκο προκειμένου να το στείλουμε στο Transmission (3).



Το Torrent που ανεβάσαμε κατεβαίνει ήδη και στο απλό web panel του Transmission υπάρχει τώρα περισσότερη δράση.



Και μιας και μιλήσαμε για δράση, επιλέγοντας ένα ενεργό torrent μπορούμε να βλέπουμε ένα πλήθος πληροφοριών που το αφορούν, όπως, π.χ., το χρόνο που απομένει για την ολοκλήρωση του download, τη λίστα με τους peers κ.ο.κ. Το Seedbox μας είναι πλέον ετοιμοπόλεμο, ωστόσο έχουμε δύο σημαντικές εκκρεμότητες που αφορούν στην προστασία της ιδιωτικότητας και της ανωνυμίας.

Ενεργοποίηση VPN tunnel, με server του TorGuard

Θέλουμε το Seedbox μας να βγαίνει στο Internet μέσω ενός OpenVPN server του TorGuard (βλ. άρθρο σελ. 14). Για τη συνέχεια υποθέτουμε ότι έχουμε λογαριασμό στο TorGuard και συγκεκριμένα ενεργή συνδρομή για την υπηρεσία Anonymous VPN. Από τη γραμμή εντολών του Seedbox μας, κατεβάζουμε το πακέτο του TorGuard με τα αρχεία ρυθμίσεων για συνδέσεις UDP προς τους servers της εταιρείας. (Μιας κι από το Seedbox κατεβάζουμε torrents και μας ενδιαφέρει η ταχύτητα, προτιμάμε να συνδεόμαστε σε OpenVPN servers μέσω UDP κι όχι μέσω TCP.)

```
sub0@seedbox:~$ wget https://torguard.net/downloads/OpenVPN-UDP.zip
```

Παίρνουμε το αρχείο OpenVPN-UDP.zip, το οποίο κι αποσυμπιέζουμε:

```
sub0@seedbox:~$ unzip OpenVPN-UDP.zip
```

Προκύπτει ο κατάλογος "OpenVPN -UDP" κι αυτό το κενό στ' όνομα μάς κάνει ν' αναρωτιόμαστε τι σκεφτόταν ο υπάλληλος της TorGuard, την ημέρα που έφτιαξε το αρχείο OpenVPN-UDP.zip. Δεν είναι απαραίτητο να απαλείψουμε το κενό, αν όμως *δεν* το κάνουμε θα συνεχίσουμε με άγχος, ανησυχία κι ενοχές. Δεν ξέρουμε για εσάς, σ' εμάς όμως δεν αρέσει ούτε το άγχος, ούτε η ανησυχία, ούτε οι ενοχές:

```
sub0@seedbox:~$ mv "OpenVPN -UDP" OpenVPN-UDP
```

Τα αρχεία εντός του καταλόγου OpenVPN-UDP είναι εκτελέσιμα, χωρίς να υπάρχει λόγος. Αλλάζουμε τα δικαιώματά τους ώστε ο ιδιοκτήτης να έχει δικαιώματα ανάγνωσης κι εγγραφής, ενώ όλοι οι άλλοι δικαίωμα ανάγνωσης:

```
sub0@seedbox:~$ chmod 644 OpenVPN-UDP/*
```

Στο σημείο αυτό εγκαθιστούμε στο Ubuntu μας το OpenVPN, το οποίο λειτουργεί είτε ως server είτε ως client:

```
sub0@seedbox:~$ sudo apt-get install openvpn
```

Μεταφέρουμε ολόκληρο τον κατάλογο OpenVPN-UDP εντός του /etc/openvpn και μεταβαίνουμε στον προαναφερθέντα:

```
sub0@seedbox:~$ sudo mv OpenVPN-UDP /etc/openvpn/TorGuard-UDP
sub0@seedbox:~$ cd /etc/openvpn
```

Όπως βλέπετε, καθώς μετακινήσαμε τον κατάλογο OpenVPN-UDP στη νέα του θέση, τον μετονομάσαμε κιόλας. Μέσα στον TorGuard-UDP υπάρχει το αρχείο ca.crt, που είναι το δημόσιο πιστοποιητικό της Αρχής Πιστοποίησης του TorGuard. Το συγκεκριμένο αρχείο το αντιγράφουμε στον κατάλογο /etc/openvpn:

```
sub0@seedbox:/etc/openvpn$ sudo cp TorGuard-UDP/ca.crt .
```

Αν ρίξουμε μια ματιά μέσα στον κατάλογο TorGuard-UDP, είναι εύκολο να καταλάβουμε σε ποιους servers αντιστοιχεί καθένα από τα αρχεία ρύθμισης του TorGuard:

```
sub0@seedbox:/etc/openvpn$ ls TorGuard-UDP
ca.crt                            TorGuard.Indonesia.ovpn     TorGuard.South.Korea.ovpn
TorGuard.Australia.Melbourne.ovpn TorGuard.Ireland.ovpn       TorGuard.Spain.ovpn
TorGuard.Australia.Sydney.ovpn    TorGuard.Italy.ovpn         TorGuard.Sweden.Stockholm.ovpn
TorGuard.Belgium.ovpn             TorGuard.Japan.ovpn         TorGuard.Swiss.ovpn
TorGuard.Brazil.ovpn              TorGuard.Latvia.ovpn        TorGuard.Thailand.ovpn
TorGuard.Canada.Calgary.ovpn      TorGuard.Luxembourg.ovpn    TorGuard.Tunisia.ovpn
TorGuard.Canada.Toronto.ovpn      TorGuard.Malaysia.ovpn      TorGuard.Turkey.ovpn
TorGuard.Canada.Vancouver.ovpn    TorGuard.Mexico.ovpn        TorGuard.UK.Hampshire.ovpn
```

```
TorGuard.Costa Rica.ovpn          TorGuard.Moldova.ovpn                TorGuard.UK.London.ovpn
TorGuard.Czech.ovpn               TorGuard.Netherlands.ovpn            TorGuard.USA-ARIZONA.ovpn
TorGuard.Denmark.ovpn             TorGuard.New.Zealand.ovpn            TorGuard.USA-ATLANTA.ovpn
TorGuard.Egypt.ovpn               TorGuard.Norway.ovpn                 TorGuard.USA-CHICAGO.ovpn
TorGuard.Finland.ovpn             TorGuard.Panama.ovpn                 TorGuard.USA-DALLAS.ovpn
TorGuard.France.ovpn              TorGuard.Poland.ovpn                 TorGuard.USA-LA.ovpn
TorGuard.Germany.Frankfurt.ovpn   TorGuard.Portugal.ovpn               TorGuard.USA-LAS-VEGAS.ovpn
TorGuard.Germany.Munich.ovpn      TorGuard.Romania.ovpn                TorGuard.USA-MIAMI.ovpn
TorGuard.Greece.ovpn              TorGuard.Russia.Moscow.ovpn          TorGuard.USA-NEW-JERSEY.ovpn
TorGuard.Hong.Kong.ovpn           TorGuard.Russia.St.Petersburg.ovpn   TorGuard.USA-NEW-YORK.ovpn
TorGuard.Hungary.ovpn             TorGuard.Saudi.Arabia.ovpn           TorGuard.USA-SEATTLE.ovpn
TorGuard.Iceland.ovpn             TorGuard.Singapore.ovpn              TorGuard.Vietnam.ovpn
TorGuard.India.ovpn               TorGuard.South.Africa.ovpn
```

Για τις ανάγκες της παρουσίασής μας, ας φροντίσουμε ώστε το Seedbox να βγαίνει στο Internet μέσω του server στην Ελβετία. Το αρχείο που θέλουμε, λοιπόν, είναι το TorGuard.Swiss.ovpn. Τώρα, προκειμένου ν' αλλάζουμε εύκολα OpenVPN server κάθε φορά που το επιθυμούμε, αλλά και για λόγους καλής διαχείρισης, αφήνουμε το αρχείο TorGuard.Swiss.ovpn μέσα στον κατάλογο /etc/openvpn/TorGuard-UDP κι από τον /etc/openvpn φτιάχνουμε ένα symbolic link προς αυτό:

```
sub0@seedbox:/etc/openvpn$ sudo ln -s TorGuard-UDP/TorGuard.Swiss.ovpn
VPNserver.conf
```

Σημειώστε ότι σκόπιμα δώσαμε στο αρχείο VPNserver την κατάληξη ".conf". Έτσι, μόλις η τοπική υπηρεσία του OpenVPN ενεργοποιηθεί θα το διαβάσει αυτόματα. Πριν τη σύνδεσή μας ανοίγουμε το αρχείο VPNserver.conf με το nano – και φυσικά με δικαιώματα διαχειριστή:

```
sub0@seedbox:/etc/openvpn$ nano VPNserver.conf
```

Τη γραμμή "auth-user-pass" την αλλάζουμε σε "auth-user-pass credentials.txt" (χωρίς τα εισαγωγικά). Αποθηκεύουμε την αλλαγή (με [CTRL+O], [Enter]) κι εγκαταλείπουμε το nano (με [CTRL+X]). Φτιάχνουμε στη συνέχεια το αρχείο credentials.txt:

```
sub0@seedbox:/etc/openvpn$ sudo nano credentials.txt
```

Το περιεχόμενό του πρέπει ν' αποτελείται από δύο γραμμές μόνο, όπου η πρώτη έχει το username και η δεύτερη το password μας στο TorGuard. Αφού αποθηκεύσουμε το αρχείο και βγούμε από το nano, φροντίζουμε ώστε δικαίωμα ανάγνωσης και εγγραφής στο credentials.txt να έχει μόνον ο χρήστης root:

```
sub0@seedbox:/etc/openvpn$ sudo chown 600 credentials.txt
```

Είμαστε πλέον έτοιμοι να συνδεθούμε στον OpenVPN server του TorGuard, στην Ελβετία. Πρώτα όμως ας σημειώσουμε το δημόσιο IP που έχει το Seedbox μας, καθώς και τον name server που χρησιμοποιεί. Για το δημόσιο IP, γράφουμε:

```
sub0@seedbox:/etc/openvpn$ curl icanhazip.com
87.203.x.x
```

Για τον name server, πληκτρολογούμε κάτι σαν

```
sub0@seedbox:/etc/openvpn$ dig deltahacker.gr
; <<>> DiG 9.9.5-3ubuntu0.7-Ubuntu <<>> deltahacker.gr
;; global options: +cmd
;; Got answer:
...
;; Query time: 75 msec
;; SERVER: 192.168.10.254#53(192.168.10.254)
;; WHEN: Sun Feb 21 14:39:58 EET 2016
;; MSG SIZE  rcvd: 59
```

Στην τρίτη γραμμή από το τέλος, βλέπουμε ότι ο name server είναι ο 192.168.10.254. Πρόκειται για τον router μπροστά από το Seedbox. Ας συνδεθούμε τώρα στον OpenVPN server του TorGuard:

```
sub0@seedbox:/etc/openvpn$ sudo service openvpn start
 * Starting virtual private network daemon(s)...
 *   Autostarting VPN 'VPNserver'
```

Αν όλα έχουν πάει καλά, τότε στην έξοδο του ifconfig πρέπει να δούμε και το tun0 interface. Δείτε:

```
sub0@seedbox:/etc/openvpn$ ifconfig

eth0      Link encap:Ethernet  HWaddr 52:54:00:e7:de:78
```

```
          inet addr:192.168.10.225  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fee7:de78/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7440054 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5923232 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17597153786 (17.5 GB)  TX bytes:5273568359 (5.2 GB)
...
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.9.0.10  P-t-P:10.9.0.9  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2976 (2.9 KB)  TX bytes:3217 (3.2 KB)
```

Όλα μοιάζουν τέλεια. Ας ελέγξουμε αν το δημόσιο IP μας έχει αλλάξει:

```
sub0@seedbox:/etc/openvpn$ curl icanhazip.com
179.43.188.214
```

Και ναι, έχει αλλάξει! Αν όμως δώσουμε ξανά "dig deltahacker.gr" (χωρίς τα εισαγωγικά), θα διαπιστώσουμε ότι συνεχίζουμε να χρησιμοποιούμε τον ίδιο name server. Το γεγονός επαληθεύεται ρίχνοντας και μια ματιά στο αρχείο /etc/resolv.conf:

```
sub0@seedbox:/etc/openvpn$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.10.254
search colder.xyz
```

Παρά λοιπόν την επιτυχημένη σύνδεσή μας στον TorGuard server, αναλόγως των name servers που χρησιμοποιεί ο router μας, ο ISP είναι πιθανό να βλέπει ποια sites επισκεπτόμαστε ή ποιες ιντερνετικές υπηρεσίες χρησιμοποιούμε. Προκειμένου ν' αποφύγουμε τα δυνητικά DNS leaks, θέλουμε ο πρώτος name server του συστήματος να είναι ο 10.9.0.1: αυτή είναι η διεύθυνση IP του απομακρυσμένου TorGuard server για το tun0 interface. Το αρχείο /etc/resolv.conf δεν έχει νόημα να το τροποποιήσουμε χειροκίνητα, διότι επαναδημιουργείται αυτόματα κατά την εκκίνηση του λειτουργικού. Μπορούμε όμως να αλλάξουμε τον τρόπο δημιουργίας του...

```
root@seedbox:/etc/openvpn# echo "nameserver 10.9.0.1" >> /etc/resolvconf/
resolv.conf.d/head
```

...και να επανεκκινήσουμε την υπηρεσία ονόματι resolvconf:

```
sub0@seedbox:/etc/openvpn$ sudo service resolvconf restart
```

Πλέον, το περιεχόμενο του /etc/resolv.conf θα έχει αλλάξει...

```
sub0@seedbox:/etc/openvpn$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.9.0.1
nameserver 192.168.10.254
search colder.xyz
```

...κι ο name server που θα απαντά στα DNS queries θα 'ναι ο 10.9.0.1:

```
sub0@seedbox:/etc/openvpn$ dig deltahacker.gr
; <<>> DiG 9.9.5-3ubuntu0.7-Ubuntu <<>> deltahacker.gr
;; global options: +cmd
;; Got answer:
...
;; Query time: 148 msec
;; SERVER: 10.9.0.1#53(10.9.0.1)
;; WHEN: Sun Feb 21 15:17:57 EET 2016
;; MSG SIZE  rcvd: 150
```

Προσοχή! Για διάφορους λόγους, ο name server στο 10.9.0.1 ενδέχεται να μην απαντά. Όταν συμβαίνει αυτό δεν θα παίρνουμε κάποιο μήνυμα λάθους, αφού θα χρησιμοποιείται ο επόμενος διαθέσιμος name server – στο παράδειγμά μας ο 192.168.10.254. Προκειμένου να μην έχουμε το φόβο των DNS leaks ως προς τον ISP μας, μια εναλλακτική είναι να φροντίσουμε ώστε στην αρχή του /etc/resolv.conf να βρίσκονται οι δύο name servers της Google, με διευθύνσεις 8.8.8.8 και 8.8.4.4.

Λογικά, στο σημείο αυτό όλα θα πρέπει να δουλεύουν όπως ακριβώς θέλουμε. Συγκεκριμένα, κατά την εκκίνηση του λειτουργικού συνδεόμαστε στον OpenVPN server του TorGuard στην Ελβετία, η διαδικτυακή μας κίνηση δρομολογείται μέσω του απομακρυσμένου server, βγαίνουμε στο Internet όχι με το δημόσιο IP που μας έχει δώσει ο ISP, είμαστε ασφαλείας κι ως προς τα DNS leaks. Επειδή κάναμε πολλή δουλειά και πειράξαμε ένα σωρό πράγματα, ίσως είναι καλή ιδέα να επανεκκικήσουμε το Seedbox μας...

```
sub0@seedbox:/etc/openvpn$ sudo reboot
```

...κι αφού ξεκινήσει και συνδεθούμε και πάλι, να κάνουμε μια-δυο δοκιμές για το δημόσιο IP μας και τον χρησιμοποιούμενο name server.

Κατέβασμα μόνο μέσω VPN

Για οποιονδήποτε λόγο, η σύνδεσή μας προς τον TorGuard server είναι πιθανό να πέσει. Αν εκείνη τη στιγμή κατεβάζουμε με το Transmission, το downloading θα σταματήσει για λίγο αλλά λίγα δευτερόλεπτα αργότερα θα συνεχίσει από το eth0 interface, άρα μέσω του ISP μας. Ξαφνικά, λοιπόν, η δραστηριότητά μας γίνεται φανερή – εκτός βέβαια κι αν έχουμε λάβει τα μέτρα μας.

Αν υπήρχε τρόπος ώστε να λέγαμε στο Transmission κάτι στο στιλ "κατέβαζε μόνο μέσω του τάδε network interface", θα του υποδεικνύαμε το tun0 και δεν θα είχαμε κανένα πρόβλημα: όσο το tun0 ήταν up θα είχαμε δυνατότητα για downloading, ενώ αν γινόταν down απλά δεν θα μπορούσαμε να κατεβάζουμε. Το θέμα είναι ότι το Transmission δεν είναι δυνατόν να δεχτεί τέτοια οδηγία. Ευτυχώς όμως που υπάρχει το iptables. Ρίχνοντας μια ματιά στις προκαθορισμένες πολιτικές του Ubuntu Server για τις αλυσίδες INPUT, FORWARD και OUTPUT, παρατηρούμε ότι δεν υπάρχει κανένας περιορισμός για καμία τους:

```
sub0@seedbox:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

Το Seedbox μας βρίσκεται πίσω από το firewall του router, δεν έχουμε κάποιον κανόνα port forwarding ώστε να φτάνουμε στο VM από τον έξω κόσμο, επομένως δεν υπάρχει λόγος ν' ασχοληθούμε με την αλυσίδα INPUT. Ούτε με την αλυσίδα FORWARD έχουμε λόγο ν' ασχοληθούμε, αφού το VM δεν λειτουργεί ως router. Μας μένει λοιπόν η αλυσίδα OUTPUT – και μ' αυτή *έχει* νόημα ν' ασχοληθούμε. Αναλυτικότερα, τα εξερχόμενα πακέτα που προορίζονται για το τοπικό δίκτυο θα τα αφήνουμε να περνούν, αλλά σε όσα προορίζονται για το Internet θα τους επιτρέπουμε την έξοδο *μόνον* όταν διέρχονται μέσα από το tun0 interface. Έτσι, όταν η σύνδεση προς τον TorGuard server πέφτει, το Seedbox μας θα μπορεί να επικοινωνεί μόνο με άλλα μη-

χανήματα ή VMs του τοπικού δικτύου. Ο ISP μας θα εξακολουθεί να είναι στα σκοτάδια ως προς τις δραστηριότητές μας, ενώ εμείς θα μπορούμε να κάνουμε ένα SSH login στο VM για να ξεκινήσουμε, ίσως, μια νέα σύνδεση VPN, ενδεχομένως προς άλλον TorGuard server.

Έχουμε ετοιμάσει ένα εξαιρετικά απλό σκριπτ, το οποίο θέτει τους προαναφερθέντες κανόνες για τα εξερχόμενα πακέτα. Κατεβάστε το πληκτρολογώντας:

```
sub0@seedbox:~$ wget -O iptables-ruleset.sh http://bit.ly/iptrs
```

Δείτε λίγο τα περιεχόμενά του:

```
sub0@seedbox:~$ cat iptables-ruleset.sh
#!/bin/bash
iptables -F
iptables -A OUTPUT --out-interface lo -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT --out-interface eth0 --destination 192.168.0.0/16 -j ACCEPT
iptables -A OUTPUT --out-interface tun0 -j ACCEPT
iptables -A OUTPUT -j DROP
```

Όπως παρατηρείτε, επιτρέπουμε την έξοδο στα πακέτα που προορίζονται προς το loopback interface, σ' εκείνα των ήδη εγκαθιδρυμένων συνδέσεων, καθώς και στα πακέτα τα οποία, μέσω του eth0, προορίζονται για άλλα μηχανήματα του τοπικού δικτύου. Επιτρέπουμε επίσης τα πακέτα που βγαίνουν έξω μέσω του tun0 interface, δηλαδή εκείνα που εξέρχονται μέσω του κρυπτογραφημένου τούνελ. Τέλος, μπλοκάρουμε όλα τα άλλα εξερχόμενα πακέτα.

Το αρχείο iptables-ruleset.sh το κάνουμε εκτελέσιμο...

```
sub0@seedbox:~$ chmod 755 iptables-ruleset.sh
```

...και το μεταφέρουμε σε έναν ωραιότατο κατάλογο, ονόματι bin, μέσα στον προσωπικό κατάλογο του χρήστη μας:

```
sub0@seedbox:~$ mkdir bin
sub0@seedbox:~$ mv iptables-ruleset.sh ~/bin/
```

Ας το εκτελέσουμε τώρα...

```
sub0@seedbox:~$ sudo ~/bin/iptables-ruleset.sh
```

...κι ας παρατηρήσουμε τους νέους κανόνες που ισχύουν:

```
sub0@seedbox:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 192.168.0.0/16 -o eth0 -j ACCEPT
-A OUTPUT -o tun0 -j ACCEPT
-A OUTPUT -j DROP
```

Με ό,τι ισχύει, από ένα οποιοδήποτε μηχάνημα του τοπικού δικτύου θα φτάνουμε στο Seedbox – και το αντίστροφο. Με την προϋπόθεση ότι έχουμε ενεργή σύνδεση σε TorGuard server, από το Seedbox θα βγαίνουμε στο Internet μέσω tun0 – αλλά όχι μέσω eth0. Τερματίζοντας μόνοι μας τη σύνδεση VPN, π.χ., πληκτρολογώντας

```
sub0@seedbox:~$ sudo service openvpn stop
 * Stopping virtual private network daemon(s)...
 *   Stopping VPN 'VPNserver'
```

θα διαπιστώσουμε ότι η επικοινωνία του Seedbox με όλες τις άλλες δικτυωμένες συσκευές του τοπικού δικτύου θα συνεχίσει να είναι δυνατή. Καταφεύγοντας όμως σε εργαλεία όπως το ping ή το mtr, θα διαπιστώσουμε ότι η πρόσβαση στο Internet εμποδίζεται. Την ίδια διαπίστωση θα κάνουμε αν προσπαθήσουμε να κατεβάσουμε κάτι με το Transmission.

Προκειμένου να ενεργοποιήσουμε και πάλι μια σύνδεση VPN, οφείλουμε πρώτα να αδειάσουμε όλους τους κανόνες του iptables:

```
sub0@seedbox:~$ sudo iptables -F
sub0@seedbox:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

Στη συνέχεια εγκαθιδρύουμε σύνδεση προς κάποιον TorGuard server...

```
sub0@seedbox:~$ sudo service openvpn start
 * Starting virtual private network daemon(s)...
 *   Autostarting VPN 'VPNserver'
```

...και φορτώνουμε ξανά το ruleset:

```
sub0@seedbox:~$ sudo ~/bin/iptables-ruleset.sh
sub0@seedbox:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 192.168.0.0/16 -o eth0 -j ACCEPT
-A OUTPUT -o tun0 -j ACCEPT
-A OUTPUT -j DROP
```

Οι κανόνες είναι βολικό να ενεργοποιούνται κατά την εκκίνηση του λειτουργικού συστήματος. Ένας τρόπος για να το πετύχουμε, είναι με την εισαγωγή μιας απλής γραμμής στο αρχείο /etc/rc.local. Δείτε το δικό μας:

```
sub0@seedbox:~$ cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
/home/sub0/bin/iptables-ruleset.sh
exit 0
```

Η γραμμή που εισαγάγαμε είναι η τονισμένη. Αν και δεν είναι απαραίτητο, προτείνουμε να επανεκκινήσετε το λειτουργικό και κατόπιν να κάνετε μερικούς ελέγχους, ώστε να διαπιστώσετε αν όλα λειτουργούν κατά τα προβλεπόμενα.

cvar — sub0@seedbox: ~ — ssh seedbox — 115×40 — ⌘1

```
sub0@seedbox:~$
sub0@seedbox:~$ sudo service openvpn status
 * VPN 'VPNserver' is running
sub0@seedbox:~$ curl icanhazip.com
179.43.173.82
sub0@seedbox:~$ ping -c 3 google.com
PING google.com (62.75.23.123) 56(84) bytes of data.
64 bytes from 62.75.23.123: icmp_seq=1 ttl=56 time=126 ms
64 bytes from 62.75.23.123: icmp_seq=2 ttl=56 time=126 ms
64 bytes from 62.75.23.123: icmp_seq=3 ttl=56 time=126 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 126.248/126.567/126.728/0.468 ms
sub0@seedbox:~$
sub0@seedbox:~$ sudo service openvpn stop
 * Stopping virtual private network daemon(s)...
 *   Stopping VPN 'VPNserver'                                                        [ OK ]
sub0@seedbox:~$ curl icanhazip.com
^C
sub0@seedbox:~$ ping -c 3 google.com
PING google.com (62.75.23.123) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- google.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2015ms

sub0@seedbox:~$ ping -c 3 thehost
PING thehost.colder.xyz (192.168.10.245) 56(84) bytes of data.
64 bytes from thehost.colder.xyz (192.168.10.245): icmp_seq=1 ttl=64 time=0.170 ms
64 bytes from thehost.colder.xyz (192.168.10.245): icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from thehost.colder.xyz (192.168.10.245): icmp_seq=3 ttl=64 time=0.175 ms

--- thehost.colder.xyz ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.170/0.178/0.189/0.008 ms
sub0@seedbox:~$
```

*Με τη σύνδεση VPN σε TorGuard server ενεργή (1), από τη γραμμή εντολών του Seedbox μας ελέγχουμε το δημόσιο IP με το οποίο βγαίνουμε στο Internet (2). Η επικοινωνία μας εξάλλου με τον έξω κόσμο, γίνεται ανεμπόδιστα (3). Στη συνέχεια τερματίζουμε τη σύνδεση VPN (4) κι αμέσως παρατηρούμε ότι τώρα δεν μπορούμε να μάθουμε το δημόσιο IP μας, π.χ., από το icanhazip.com (5). Ούτε το ping προς το Google δουλεύει (6), μπορούμε όμως να φτάνουμε σε άλλα μηχανήματα του τοπικού μας δικτύου (7). Όλα αυτά οφείλονται στους απλούς κανόνες του iptables που έχουμε θέσει σε ισχύ: Όσο είμαστε συνδεδεμένοι σε TorGuard server στο Internet βγαίνουμε χωρίς προβλήματα, αν όμως η σύνδεση για οποιονδήποτε λόγο διακοπεί, τότε το Seedbox μας μπορεί να επικοινωνεί *μόνο* με άλλα μηχανήματα του τοπικού δικτύου.*

Skill: Beginner
Tags: Active Directory, Domain Controller, Windows, Linux, Kerberos, SMB, CIFS, Samba

Υπηρεσίες Active Directory, χωρίς active-τσέπη

[μέρος 2/2]

Τα θεμέλια του οικοδομήματός μας είναι στιβαρά. Από μόνα τους όμως δεν προσφέρουν τίποτα χρήσιμο. Σε αυτό το δεύτερο μέρος θα συνεχίσουμε την εργασία μέχρι την ολοκλήρωση και της τελευταίας λεπτομέρειας. Μη νομίσετε πάντως ότι θα μπλέξουμε σε δύσκολα μονοπάτια. Θα εξακολουθήσουμε να χρησιμοποιούμε μικρά και εύχρηστα εργαλεία.

του Πέτρου Κυλαδίτη

Στο τέλος του πρώτου μέρους, που ξεκινά από τη σελίδα 28, καταφέραμε να στήσουμε τον δικό μας Domain Controller. Θα μπορούσαμε τώρα να ξεκινήσουμε την προσπάθεια σύνδεσης των συστημάτων αλλά, όπως συμβαίνει στις περισσότερες περιπτώσεις, η βιασύνη δεν αποτελεί καλό σύμβουλο. Για αρχή, μπορούμε να κάνουμε μια ακόμα επανεκκίνηση και στη συνέχεια να τσεκάρουμε τις ρυθμίσεις και τη λειτουργικότητα του Samba server. Για την επανεκκίνηση δεν χρειάζεται να πούμε πολλά:

```
$ sudo reboot
```

Όταν συνδεθούμε ξανά στο σύστημα, μπορούμε να αρχίσουμε τους ελέγχους. Όσοι άφησαν ενεργά όλα τα μέτρα ασφαλείας του κωδικού του διαχειριστή, μπορούν να τσεκάρουν το χρονικό διάστημα που απομένει μέχρι τη λήξη του. Για το σκοπό αυτό χρησιμοποιούμε το kinit – ένα πρόγραμμα που συνοδεύει την υπηρεσία Kerberos:

```
$ kinit administrator@DELTA.LOCAL
```

Μόλις το τρέξουμε θα μας ζητηθεί ο κωδικός που ορίσαμε για το διαχειριστή και μόλις τον εισάγουμε, θα μάθουμε πότε λήγει. Ακολούθως, βλέπουμε αν και ποια tickets πιστοποίησης έχει εκδώσει το Kerberos. Για αυτή τη δουλειά χρησιμοποιούμε το εργαλείο klist:

```
$ klist
```

Προφανώς, εφόσον δεν έχουμε συνδέσει ακόμα κανένα σύστημα στο Domain, δεν θα έχει εκδοθεί κανένα πιστοποιητικό. Ωστόσο, τρέχοντας αυτά τα δύο προγράμματα κι από τη στιγμή που δεν εμφανίζονται μηνύματα λάθους, βεβαιωνόμαστε ότι το Kerberos λειτουργεί κανονικά. Για την επιβεβαίωση της λειτουργίας του Samba server χρησιμοποιούμε το εργαλείο smbclient:

```
$ smbclient -L localhost -U%
$ smbclient //localhost/netlogon –U 'Administrator' -c 'ls'
```

Με την εκτέλεση της πρώτης γραμμής εμφανίζονται πληροφορίες για τους πόρους και μερικές βασικές ρυθμίσεις του Samba server. Με την εκτέλεση της δεύτερης, το σύστημα θα ζητήσει να εισάγουμε τον κωδικό του διαχειριστή. Εφόσον το κάνουμε, θα προβάλει όλα τα αρχεία που ανήκουν στο συγκεκριμένο χρήστη και διαμοιράζονται από τον Samba server. Εν ολίγοις, θα εμφανιστεί κάτι που θα μοιάζει με άδειο κατάλογο. Όπως αντιλαμβάνεστε, το σκεπτικό μας παραμένει ίδιο: Αν δεν εμφανιστεί κάποιο μήνυμα λάθους, ο Samba server λειτουργεί κανονικά και είναι έτοιμος να αρχίσει το διαμοιρασμό αρχείων.

Διαμοιρασμός αρχείων

Στην εισαγωγή του προηγούμενου μέρους, τονίσαμε ότι μια μεγάλη ευκολία του Active Directory σχετίζεται με τα roaming profiles, δηλαδή τη δυνατότητα να έχουμε τα αρχεία και τις ρυθμίσεις μας σε οποιοδήποτε μηχάνημα του domain κι αν καθίσουμε. Σε ένα δίκτυο που αξιοποιεί την εν λόγω τεχνολογία, τα αρχεία που σχετίζονται με τον λογαριασμό μας δεν είναι υποχρεωτικό να βρίσκονται στον Domain controller. Μπορούν κάλλιστα να διατηρούνται σε ξεχωριστό μηχάνημα, που εκτελεί χρέη file server. Τις περισσότερες φορές πάντως τα δύο παραπάνω καθήκοντα (domain controller και file server) ανατίθενται στο ίδιο μηχάνημα. Το ίδιο θα κάνουμε κι εμείς, εφόσον έτσι μπορούμε να εξοικονομήσουμε ακόμα περισσότερους πόρους. Το γεγονός ότι ο Domain controller τρέχει Ubuntu Server και οι δίσκοι του είναι διαμορφωμένοι με το σύστημα Ext4, δεν πρέπει να σας ανησυχεί. Ο Samba server φροντίζει να μεταφέρει τα αρχεία μας από και προς τα μηχανήματα που τρέχουν Windows, χωρίς το παραμικρό πρόβλημα. Το επόμενο βήμα, λοιπόν, είναι η δημιουργία ενός κοινόχρηστου δικτυακού πόρου, στον οποίο θα φυλάσσονται τα αρχεία των χρηστών. Εντελώς αυθαίρετα, αποφασίσαμε ότι ο σχετικός αποθηκευτικός χώρος θα βρίσκεται στη θέση /home/Users:

```
$ sudo mkdir /home/Users
$ sudo chown root:users /home/Users
$ sudo chmod ug+rwx,o= /home/Users
$ sudo chmod g+s /home/Users
```

Πιστεύουμε ότι η πρώτη εντολή δεν χρειάζεται ιδιαίτερη επεξήγηση. Η δεύτερη ορίζει τον ιδιοκτήτη (owner) και την ομάδα χρηστών (user group) που ανήκει ο κατάλογος /home/Users. Ούτε κι εδώ χρειάζεται να πούμε περισσότερα. Η τρίτη εντολή όμως είναι πιθανό να σας προβληματίσει. Με αυτήν εξασφαλίζουμε ότι ο ιδιοκτήτης του καταλόγου (u), καθώς και όσοι χρήστες ανήκουν στο ίδιο group με τον κατάλογο (g), θα έχουν πλήρη πρόσβαση (+rwx). Ταυτόχρονα, οι υπόλοιποι χρήστες (o) δεν θα έχουν κανένα δικαίωμα επί του καταλόγου. Η τέταρτη εντολή τροποποιεί πάλι τα δικαιώματα του καταλόγου /home/Users και πετυχαίνει κάτι που ενδέχεται να σας ήταν εντελώς άγνωστο. Εδώ ενεργοποιούμε μια ιδιότητα που ονομάζεται setgid, από το set group ID upon execution. Η συγκεκριμένη ιδιότητα έχει άλλη ερμηνεία όταν ενεργοποιείται σε απλά αρχεία και διαφορετική όταν ενεργοποιείται σε καταλόγους. Στη δική μας περίπτωση (εφαρμογή σε κατάλογο) έχει το εξής αποτέλεσμα: Οποιοδήποτε αρχείο δημιουργείται εντός του συγκεκριμένου καταλόγου, θα ανήκει εξ ορισμού στην ομάδα χρηστών (user group) που ανήκει και ο κατάλογος. Με αυτό το τελευταίο βήμα, εξασφαλίζουμε ότι κάθε αρχείο που δημιουργεί ο Samba server μέσα στον κατάλογο /home/Users, θα ανήκει στο group ονόματι users.

Έχοντας ετοιμάσει τον κατάλογο που θα φιλοξενεί τα διαμοιραζόμενα αρχεία, πρέπει να ενημερώσουμε κατάλληλα τις ρυθμίσεις του Samba server. Έτσι, θα χρησιμοποιήσουμε τον αγαπημένο μας text editor και θα ανοίξουμε το αρχείο /etc/samba/smb.conf:

```
$ sudo nano /etc/samba/smb.conf
```

Τώρα πρέπει να μεταβούμε στο τέλος του αρχείου και να προσθέσουμε μια νέα ενότητα (section). Όπως υποψιάζεστε, εδώ θα περιγράψουμε τον κοινόχρηστο αποθηκευτικό χώρο που θέλουμε να δημιουργήσουμε:

```
[Users]
      read only = no
      path = /home/Users
      csc policy = documents
```

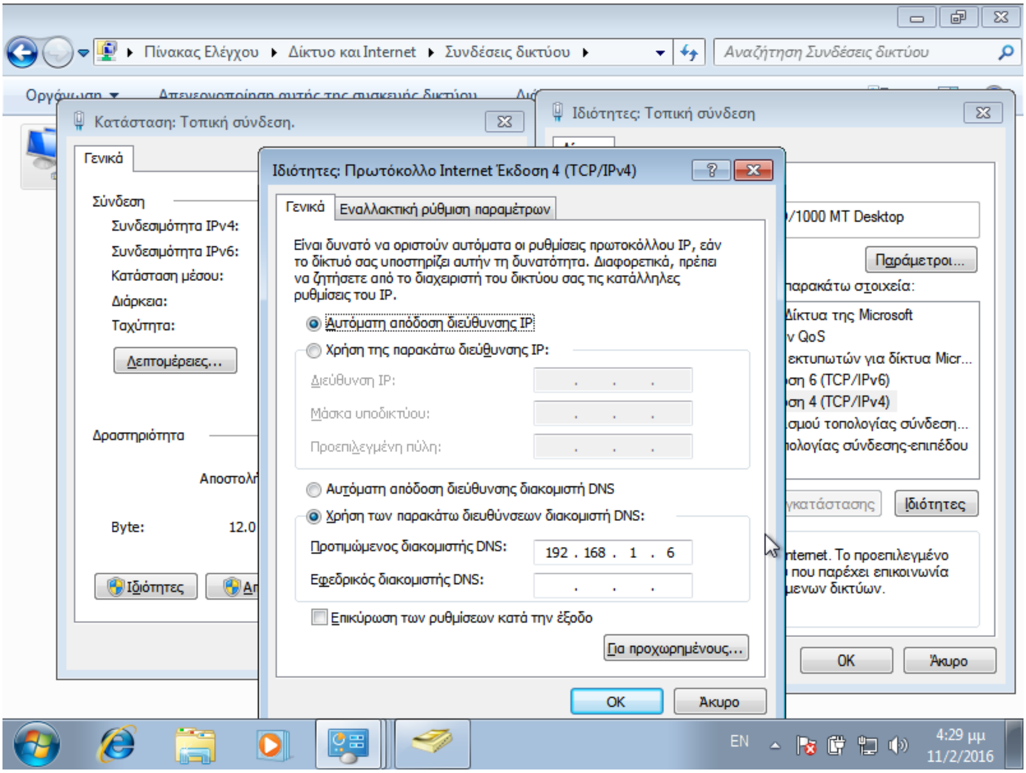
Μέσα στις αγκύλες, που ορίζουν και την έναρξη του section, τοποθετούμε το όνομα του κοινόχρηστου πόρου. Με το ίδιο όνομα θα εμφανίζεται αργότερα και στους χρήστες του Domain. Εμείς αποφασίσαμε να χρησιμοποιήσουμε το κοινότοπο αλλά άκρως κατατοπιστικό όνομα Users. Έτσι ο συγκεκριμένος πόρος θα είναι προσβάσιμος από ολόκληρο το τοπικό δίκτυο, στη θέση \\samba\Users\. Μετά από αυτή την προσθήκη, αποθηκεύουμε το αρχείο, κλείνουμε τον editor και πραγματοποιούμε μια επανεκκίνηση της υπηρεσίας Samba:

```
$ sudo service smbd restart
```

Μπορεί να μην έχετε συνειδητοποιήσει τι πετύχαμε με τα απλά βήματα που είδαμε ως τώρα, αλλά εμείς ενθουσιαστήκαμε αρκετά σε αυτή τη φάση. Στο νου μας ήρθαν στιγμές σαν αυτές που τελειώναμε μια πίστα του Super Mario και περνούσαμε στην επόμενη :D

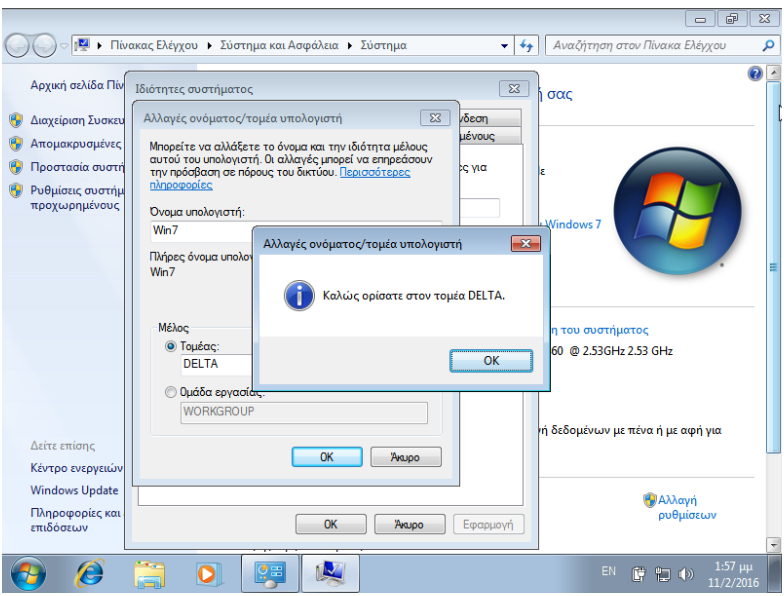
Ένταξη στο domain

Τώρα μπορούμε να μεταβούμε στα μηχανήματα που τρέχουν Windows, για να τα προσθέσουμε στο domain. Εδώ πρέπει να σας θυμίσουμε ότι μόνο οι εκδόσεις Professional (και Ultimate στην περίπτωση των Windows 7) μπορούν να ενταχθούν σε domain. Ένας τρόπος να εξασφαλίσουμε ότι το εκάστοτε σύστημα θα δει αμέσως τον Domain Controller, είναι να εξασφαλίσουμε ότι χρησιμοποιεί τον δικό μας Name server. Αυτό επιτυγχάνεται από τις ρυθμίσεις του πρωτοκόλλου TCP/IP. Στα Windows 7, για παράδειγμα, πρέπει να ανοίξουμε το "Κέντρο δικτύου", να πατήσουμε στο "Αλλαγή ρυθμίσεων προσαρμογέα" κι από 'κεί, να κάνουμε διπλό κλικ επάνω στο εικονίδιο που αναπαριστά την ενεργή κάρτα δικτύου του υπολογιστή. Στο παράθυρο που εμφανίζεται πατάμε το κουμπί "Ιδιότητες" και στο νέο παράθυρο κάνουμε διπλό κλικ στο πρωτόκολλο TCP/IP 4. Έτσι εμφανίζεται ένα ακόμα παράθυρο, στο οποίο ορίζουμε σαν DNS address τη διεύθυνση του Domain controller μας. Στη δική μας περίπτωση δώσαμε το 192.168.1.5.



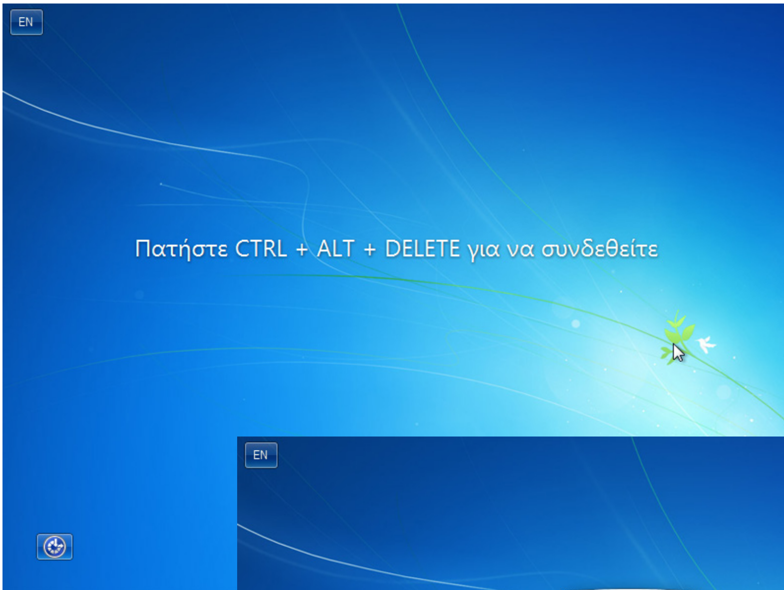
Για τον ευκολότερο εντοπισμό του Domain controller από το σύστημα, πρέπει να αλλάξουμε τη διεύθυνση του DNS. Για την ακρίβεια, πρέπει να δώσουμε τη διεύθυνση IP που έχει ο δικός μας server.

Προφανώς, επόμενο βήμα είναι η ένταξη του μηχανήματος στο domain. Αυτό μπορεί να γίνει από την ενότητα "Σύστημα" του πίνακα ελέγχου. Ένας γρήγορος τρόπος για να επισκεφθούμε τη συγκεκριμένη περιοχή, είναι να κάνουμε δεξί κλικ στο εικονίδιο "Υπολογιστής" και να επιλέξουμε τις "Ιδιότητες". Στη συνέχεια κάνουμε κλικ στο "Αλλαγή ρυθμίσεων", που εμφανίζεται λίγο παραδίπλα από το όνομα του υπολογιστή. Έτσι εμφανίζεται ένα ακόμα παράθυρο. Από εκεί μπορούμε να αλλάξουμε το όνομα του υπολογιστή και, το σημαντικότερο, να τον εντάξουμε σε κάποιο domain. Για το σκοπό αυτό πατάμε το κουμπί "Αλλαγή..." κι εμφανίζεται ένα ακόμα παράθυρο (ουφ!). Εκεί ενεργοποιούμε την επιλογή "Τομέας", αντί του "Ομάδα Εργασίας" και εισάγουμε στο σχετικό πεδίο το όνομα του Domain controller μας. Σημειώστε ότι το όνομα πρέπει να γραφεί με κεφαλαία. Για παράδειγμα εμείς δώσαμε το DELTA. Μόλις πατήσουμε το κουμπί OK, εμφανίζεται ένα παράθυρο σύνδεσης που ζητάει όνομα χρήστη και κωδικό πρόσβασης. Εκεί χρησιμοποιούμε σαν username το Administrator και τον αντίστοιχο κωδικό, που επιλέξαμε κατά την αρχική ρύθμιση του Samba server. Αν εισάγουμε τα σωστά στοιχεία, θα εμφανιστεί ένα μήνυμα καλωσορίσματος στο domain!

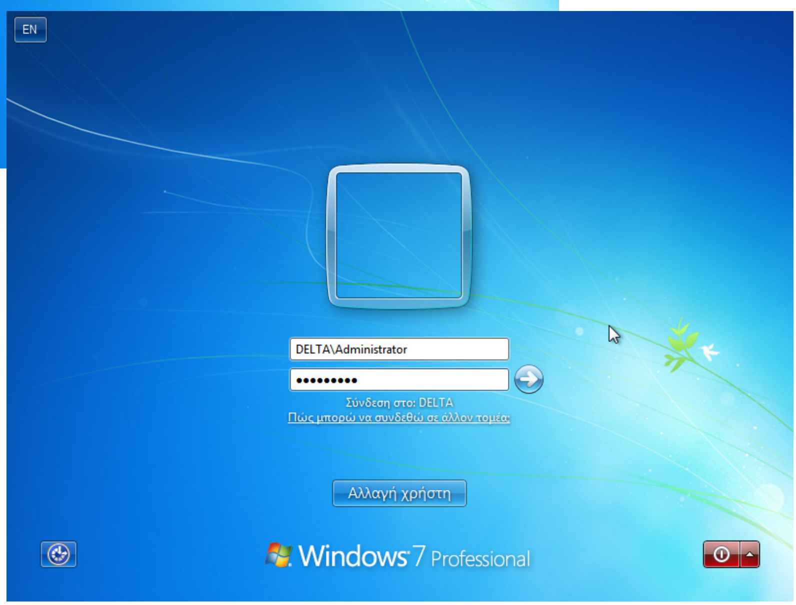


Μόλις εντάξαμε το συγκεκριμένο μηχάνημα στο domain DELTA. Στην επόμενη επανεκκίνηση θα μπορούμε να συνδεθούμε χρησιμοποιώντας λογαριασμούς χρήστη του domain.

Σε αυτό το στάδιο, για να ολοκληρωθεί η διαδικασία σύνδεσης απαιτείται μια επανεκκίνηση του υπολογιστή. Όταν ξεκινήσει το σύστημα ξανά, θα παρατηρήσετε μια σημαντική διαφορά: Η οθόνη σύνδεσης (login screen) θα είναι διαφορετική και θα σας προτρέπει να πατήσετε το συνδυασμό Ctrl+Alt+Del, για να εμφανιστεί η φόρμα σύνδεσης. Περιττό να πούμε ότι η οθόνη σύνδεσης θα εμφανιστεί ακόμα κι αν την είχατε απενεργοποιήσει, πριν από την σύνδεση στο domain.



Μετά την ένταξη στο domain, για τη σύνδεση στον υπολογιστή πρέπει να πατήσουμε το συνδυασμό πλήκτρων Ctrl+Alt+Del.



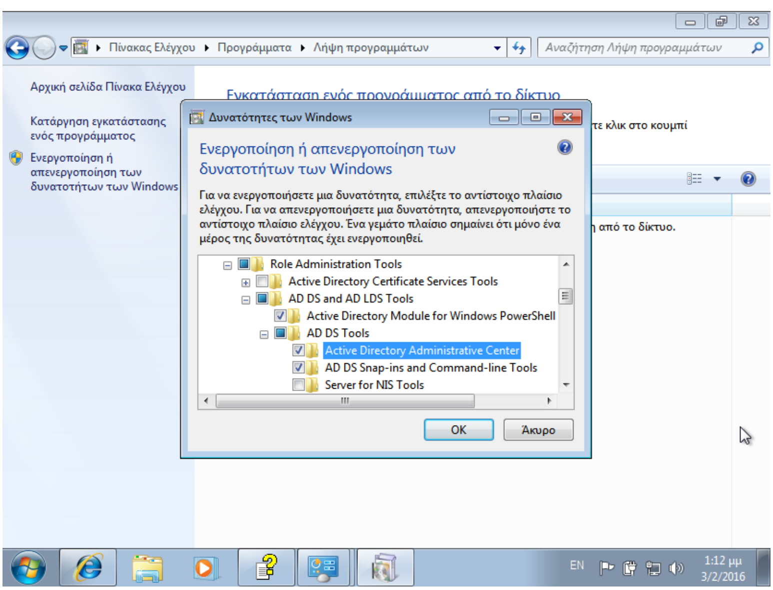
Εδώ επιχειρούμε να συνδεθούμε στο λογαριασμό Administrator του domain DELTA. Αυτός ο Administrator αποτελεί διαφορετικό χρήστη από τον Administrator που ενδέχεται να προϋπήρχε στο σύστημα. Μιλάμε για τον διαχειριστή ολόκληρου του domain!

Οι δικτυακοί λογαριασμοί (αυτοί που διαχειρίζεται ο Domain Controller) έχουν σαν πρόθεμα το όνομα του domain, ενώ οι τοπικοί λογαριασμοί (αυτοί που είχαν δημιουργηθεί στο ίδιο το σύστημα), έχουν σαν πρόθεμα το όνομα του μηχανήματος. Στη δική μας περίπτωση πληκτρολογήσαμε σαν όνομα χρήστη το DELTA\Administrator και δώσαμε πάλι τον κωδικό πρόσβασης που γνωρίζει ο Samba server. Μη νομίζετε όμως ότι συνδεθήκαμε αμέσως. Καθώς ήταν η πρώτη φορά που χρησιμοποιούσαμε το συγκεκριμένο λογαριασμό, τα Windows έπρεπε να δημιουργήσουν μια επιφάνεια εργασίας με όλα τα αρχεία που διαθέτουν οι νέοι λογαριασμοί. Όταν πραγματοποιηθεί η σύνδεση και βρεθούμε στο desktop, διαπιστώνουμε ότι μπορούμε να προσθαφαιρέσουμε προγράμματα και να αλλάξουμε κάθε ρύθμιση του συστήματος. Αυτό δεν πρέπει να σας κάνει εντύπωση. Μπορεί να μη χρησιμοποιήσαμε το λογαριασμό διαχειριστή του συγκεκριμένου μηχανήματος, αλλά συνδεθήκαμε ως ο διαχειριστής ολόκληρου του domain!

Διαχείριση χρηστών

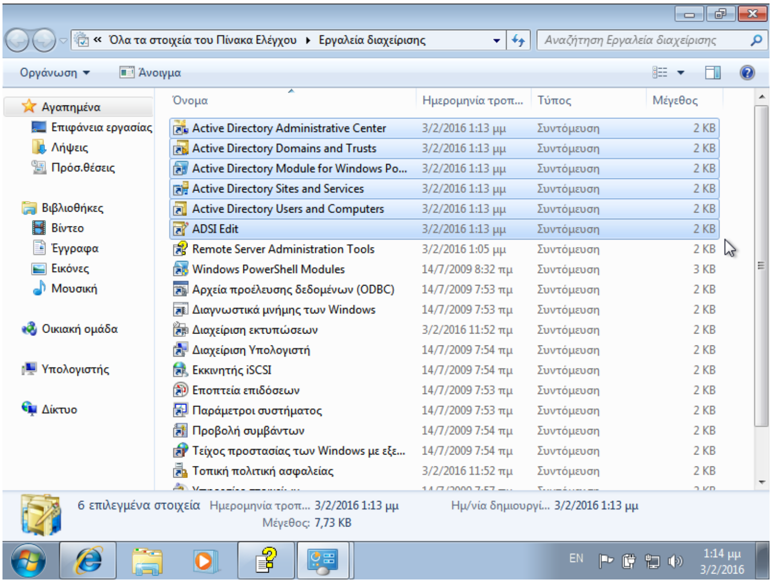
Εκτός από τον βασιλιά, ένα βασίλειο χρειάζεται και υπηκόους. Ομοίως, εκτός από τον Administrator, το domain που έχουμε στήσει χρειάζεται και απλούς χρήστες, που θα απολαμβάνουν τις υπηρεσίες του Domain controller και του δικτύου (κάτι για το οποίο δεν είμαστε σίγουροι ότι συμβαίνει με τους υπηκόους ενός βασιλείου). Η δημιουργία χρηστών μπορεί να πραγματοποιηθεί με το εργαλείο samba-tool. Ωστόσο, στο ξεκίνημα του άρθρου υποσχεθήκαμε έναν εύκολο τρόπο διαχείρισης του Active Directory. Και μπορεί το samba-tool να μην είναι στριφνό στο χειρισμό, αλλά υπάρχει κάτι πολύ πιο εύχρηστο και φιλικό. Αναφερόμαστε σ' ένα πακέτο εργαλείων που παρέχει η Microsoft και ονομάζεται "Remote Server Administration Tools". Το συγκεκριμένο πακέτο διατίθεται δωρεάν για όλες τις εκδόσεις των Windows, από τα XP έως τα 10. Οι αντίστοιχες εκδόσεις του πακέτου βρίσκονται στο Download Center της εταιρείας, στα ακόλουθα URLs:

Windows 10	https://www.microsoft.com/en-us/download/details.aspx?id=45520
Windows 8.1	https://www.microsoft.com/en-us/download/details.aspx?id=39296
Windows 8	https://www.microsoft.com/en-us/download/details.aspx?id=28972
Windows 7 SP1	https://www.microsoft.com/en-us/download/details.aspx?id=7887
Windows Vista	https://www.microsoft.com/en-us/download/details.aspx?id=21090
Windows XP	https://www.microsoft.com/en-ca/download/details.aspx?id=16770



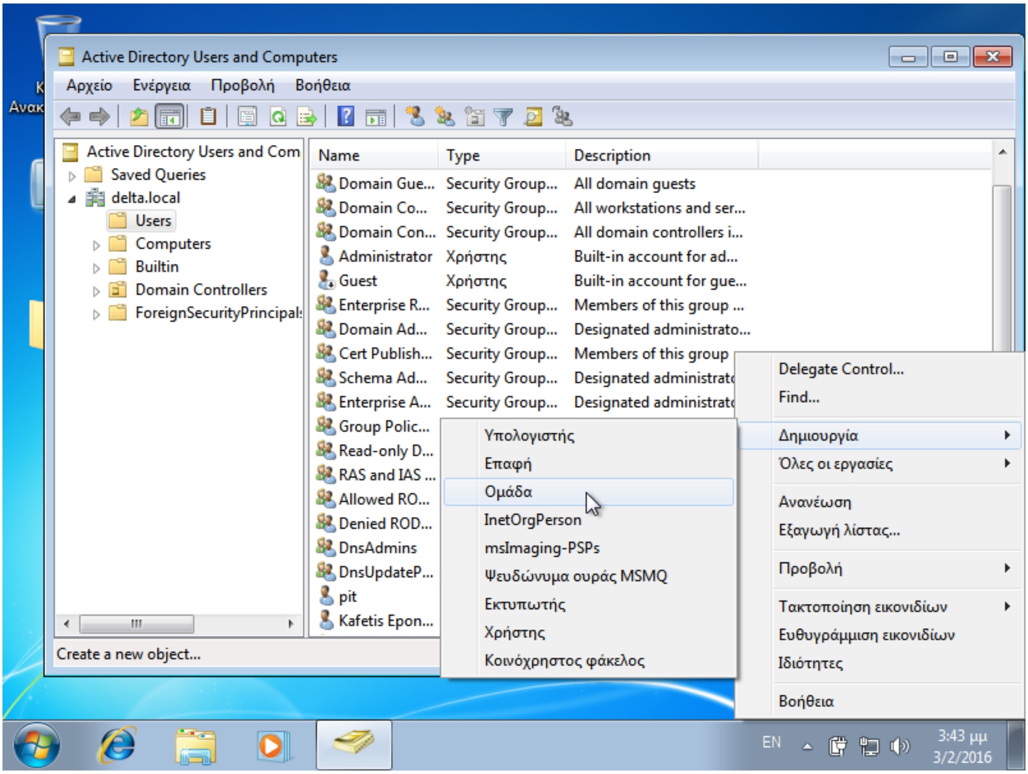
Μετά την εγκατάσταση του πακέτου των "Remote Server Administration Tools", πρέπει να προβούμε και στην ενεργοποίηση των αντίστοιχων δυνατοτήτων.

Έχετε υπόψη ότι η εγκατάσταση του συγκεκριμένου πακέτου δεν μοιάζει με την εγκατάσταση μιας τυπικής εφαρμογής. Θυμίζει περισσότερο την προσθήκη ενός πακέτου αναβάθμισης κι αν αμέσως μετά την εγκατάσταση αναζητήσετε κάτι νέο στα προγράμματα, δεν θα βρείτε τίποτα καινούριο! Αυτό δεν πρέπει να σας ανησυχήσει. Το πακέτο εγκαθίσταται σαν μια πρόσθετη δυνατότητα του λειτουργικού συστήματος και θα πρέπει πρώτα να την ενεργοποιήσουμε. Για το σκοπό αυτό μεταβαίνουμε στην ενότητα "Προγράμματα και Δυνατότητες" του "Πίνακα Ελέγχου" κι επιλέγουμε το "Ενεργοποίηση ή απενεργοποίηση δυνατοτήτων των Windows". Από το δέντρο των δυνατοτήτων πρέπει να εντοπίσουμε και να ενεργοποιήσουμε το στοιχείο "Active Directory Administrative Center". Μετά από αυτό το βήμα, αν επισκεφθούμε τα "Εργαλεία Διαχείρισης" του "Πίνακα Ελέγχου", θα διαπιστώσουμε με χαρά ότι έχουν προστεθεί καινούρια εργαλεία.



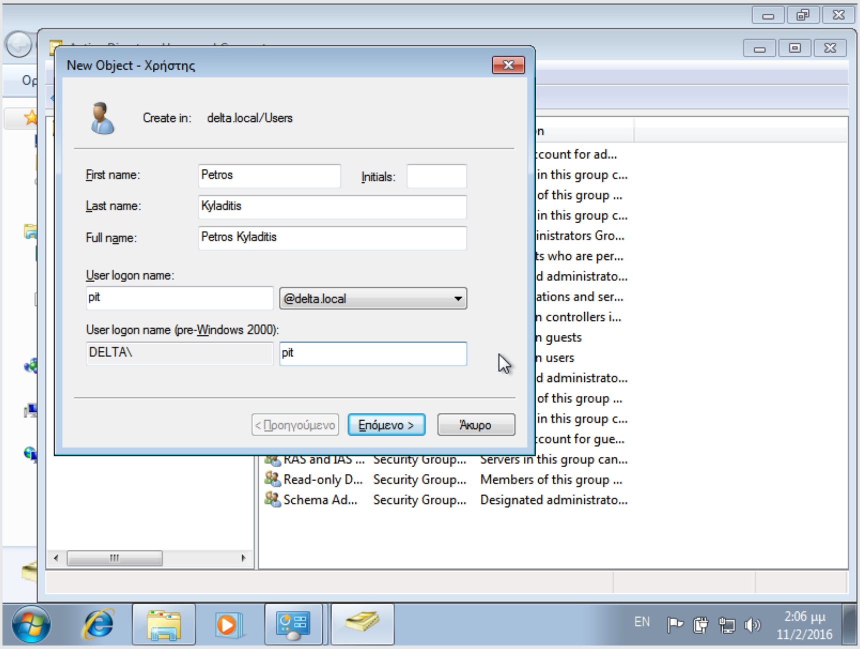
Εφόσον τα ενεργοποιήσουμε, τα εργαλεία που προσθέτει το πακέτο "Remote Server Administration Tools" εμφανίζονται στην ενότητα "Εργαλεία διαχείρισης" του "Πίνακα Ελέγχου".

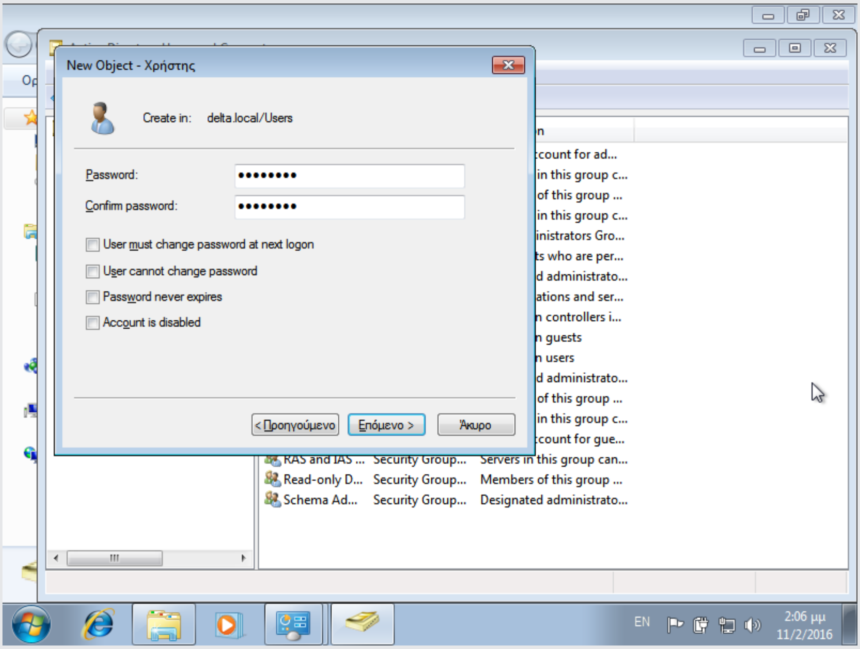
Για την προσθήκη νέων χρηστών στο domain χρειαζόμαστε το εργαλείο "Active Directory Users & Computers". Μόλις το τρέξουμε θα εμφανιστεί ένα παράθυρο και στο αριστερό του τμήμα θα δούμε ένα στοιχείο με το όνομα του domain μας. Σε αυτή τη θέση εμείς συναντήσαμε το "delta.local". Με ένα κλικ στο όνομα του domain, ξεδιπλώνεται από κάτω ένα δέντρο επιλογών. Επιλέγοντας από εκεί Users, στο δεξιό τμήμα του παραθύρου θα εμφανιστεί μια λίστα με τους χρήστες και τις ομάδες που υπάρχουν ήδη στο domain. Για να δημιουργήσουμε έναν νέο χρήστη, κάνουμε δεξί κλικ και επιλέγουμε το "Δημιουργία Χρήστη". Αυτό θα έχει σαν συνέπεια την εμφάνιση ενός μικρού οδηγού. Μη φανταστείτε κανέναν ενοχλητικό "Μάγο", με ατελείωτα περιττά βήματα, που θα μας ζητά να πατάμε διαρκώς το κουμπί "Επόμενο". Ο οδηγός που εμφανίζεται περιλαμβάνει μόλις δύο βήματα και ζητάει τα απολύτως απαραίτητα (όνομα χρήση και username, κωδικό κ.ά).



Με τη βοήθεια του "Active Directory Users & Computers" μπορούμε να δημιουργήσουμε νέους χρήστες και ομάδες χρηστών ή να αλλάξουμε τις ρυθμίσεις αυτών που υπάρχουν ήδη.

Μόλις ολοκληρώσουμε τα βήματα του οδηγού, ο νέος λογαριασμός θα εμφανιστεί στη λίστα με τους υπάρχοντες. Από εκεί, πλέον, μπορούμε να τροποποιήσουμε περισσότερες ρυθμίσεις αναφορικά με το συγκεκριμένο χρήστη. Αρκεί να κάνουμε διπλό κλικ επάνω στο όνομά του. Το παράθυρο που εμφανίζεται περιλαμβάνει πολλές καρτέλες, με πάμπολλες ρυθμίσεις που δεν θα είχε νόημα να αραδιάσουμε εδώ. Ενδιαφέρον παρουσιάζει η καρτέλα "Member Of", από την οποία μπορούμε να ορίσουμε τις ομάδες χρηστών (user groups) στις οποίες συμμετέχει ο χρήστης. Η χρήση των ομάδων επιτρέπει στον Adinistrator να διαχειρίζεται τα δικαιώματα πρόσβασης πολλών χρηστών ταυτόχρονα, χωρίς να επαναλαμβάνει τις ίδιες και τις ίδιες ρυθμίσεις, για τον καθένα ξεχωριστά. Τέλος, ιδιαίτερο ενδιαφέρον παρουσιάζει και η καρτέλα "Profile". Από εκεί μπορούμε να ενεργοποιήσουμε τη λειτουργία Roaming Profile για το συγκεκριμένο χρήστη. Για να πετύχουμε κάτι τέτοιο, πρέπει να ορίσουμε ένα δικτυακό φάκελο, στον οποίο θα αποθηκεύονται τα αρχεία και οι ρυθμίσεις του χρήστη. Αναφερόμαστε στο λεγόμενο "Profile Path". Εμείς, για τον λογαριασμό Administrator ορίσαμε τον κατάλογο \\samba\Users\Administrator. Να θυμίσουμε ότι samba είναι το hostname του Domain controller μας, ενώ Users είναι το όνομα που δώσαμε στο δικτυακό πόρο που εξυπηρετεί ο Samba server και βρίσκεται στη θέση /home/Users, του server. Εκεί μέσα δεν υπάρχει κατάλογος Administrator αλλά, όπως υποψιάζεστε, θα δημιουργηθεί αυτόματα από τον Domain controller.

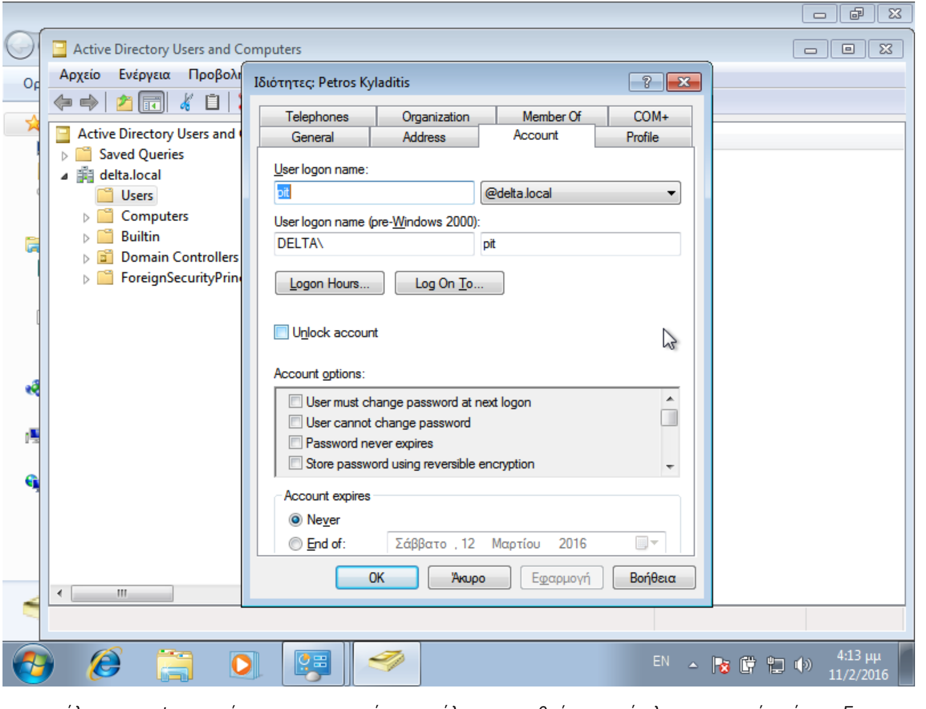




Μέσα από τα δύο βήματα που περιλαμβάνει ο σχετικός οδηγός,
η δημιουργία ενός νέου λογαριασμού χρήστη αποτελεί πανεύκολη διαδικασία.

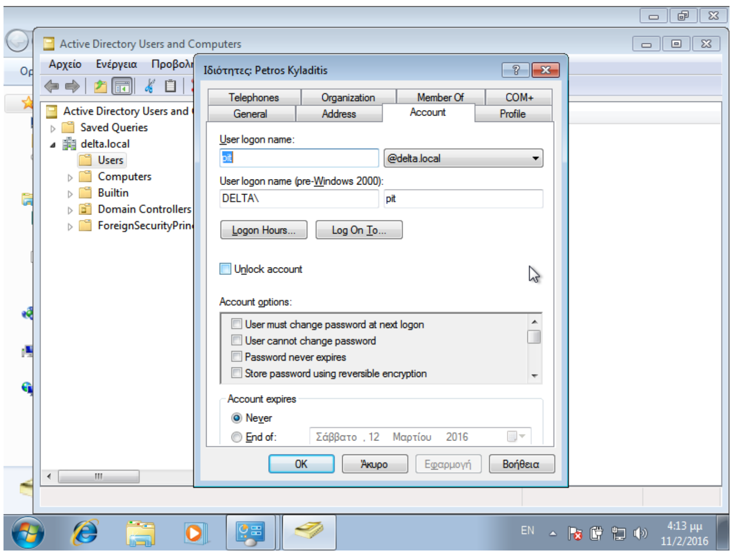
Ολοκληρώνοντας…

Τώρα μπορούμε να αποσυνδεθούμε από το μηχάνημα με τα Windows και να συνδεθούμε ξανά στον server, για να δούμε τι συνέβη όλη αυτή την ώρα. Εμείς μεταβήκαμε στον κατάλογο /home/Users, εκτελέσαμε το ls και διαπιστώσαμε ότι είχε δημιουργηθεί ένας κατάλογος ονόματι "Administrator.V2". Μέσα σε αυτόν υπήρχαν οι κατάλογοι AppData, Έγγραφα, Εικόνες, Λήψεις, Desktop και κάθε άλλο αρχείο που περιλαμβάνεται σε έναν λογαριασμό χρήστη στα Windows. Πριν προχωρήσουμε, αξίζει να σταθούμε σε μια λεπτομέρεια. Αναρωτιέστε από πού προήλθε η κατάληξη ".V2"; Όταν ορίσαμε τη θέση αποθήκευσης των αρχείων για το συγκεκριμένο λογαριασμό χρήστη, δεν δώσαμε τίποτα τέτοιο. Όπως υποψιάζεστε, το ".V2" προστέθηκε αυτόματα από τον Domain controller. Βλέπετε, κατά τη μετάβαση από τα Windows XP στα Windows Vista, το περιεχόμενο και η διάρθρωση των καταλόγων των χρηστών άλλαξαν αρκετά. Η κατάληξη ".V2", λοιπόν, χρησιμοποιείται για να αποφεύγονται τα μπερδέματα μεταξύ των διαφόρων εκδόσεων των Windows. Όταν ένας λογαριασμός χρήστη του domain συνδέεται σε σύστημα με Vista ή κάτι μεταγενέστερο, χρησιμοποιείται ο κατάλογος με την επέκταση. Αντίθετα, όταν ο ίδιος λογαριασμός χρησιμοποιείται σε σύστημα με Windows XP, τα αρχεία φυλάσσονται στον κατάλογο χωρίς την επέκταση. Εμείς είχαμε κάνει τις δοκιμές μας από ένα σύστημα με Windows 7 και ακριβώς γι' αυτό είχε προστεθεί η επέκταση. Αν είχαμε συνδεθεί από κάποιο σύστημα με Windows XP, ο κατάλογος με τα αρχεία του χρήστη θα είχε το όνομα "Administrator" – σκέτο.



Από την καρτέλα account μπορούμε να τροποποιήσουμε όλες τις ρυθμίσεις ενός λογαριασμού χρήστη. Για παράδειγμα, μπορούμε να καθορίσουμε τα μηχανήματα από τα οποία θα επιτρέπεται η σύνδεση – ή ακόμα και να την περιορίσουμε σε συγκεκριμένα "χρονικά παράθυρα" της ημέρας.

Με την υποδομή που έχουμε συγκροτήσει μπορούμε να φτιάξουμε κι άλλους κοινόχρηστους φακέλους, πέρα από αυτούς που αξιοποιεί ο Domain controller και για κάθε χρήστη. Για παράδειγμα, μπορούμε να φτιάξουμε έναν κατάλογο στον οποίο θα έχουν πρόσβαση όλοι οι χρήστες και θα τον χρησιμοποιούν για τον ελεύθερο διαμοιρασμό αρχείων. Το πώς μπορούμε να δημιουργήσουμε έναν κοινόχρηστο πόρο το είδαμε νωρίτερα. Αρκεί να φτιάξουμε έναν κατάλογο, να του δώσουμε τα επιθυμητά δικαιώματα πρόσβασης και στη συνέχεια να ενημερώσουμε κατάλληλα τον Samba server. Αυτό προϋποθέτει να προσθέσουμε μια ακόμα ενότητα, σαν αυτή που είδαμε παραπάνω, με τον τίτλο [Users].



Η καρτέλα profile μοιάζει σχεδόν αδιάφορη, αλλά διαθέτει μια ρύθμιση που ενεργοποιεί τη δυνατότητα του Roaming Profile για τον επιλεγμένο χρήστη. Αρκεί να δηλώσουμε έναν κατάλογο, σε κάποιο διαμοιραζόμενο δικτυακό πόρο.

Πραγματοποιήσαμε εκτεταμένες δοκιμές στο τοπικό μας δίκτυο και μείναμε απόλυτα ικανοποιημένοι. Μάλιστα, ο γράφων έχει αρκετή εμπειρία από τη διαχείριση δικτύων που βασίζονται σε Windows Server και οφείλει να σημειώσει ότι ο συνδυασμός Kerberos με Samba φαίνεται να λειτουργεί ταχύτερα και ομαλότερα. Τελικά, ακόμα κι αν έχετε ένα δίκτυο με μηχανήματα που τρέχουν Windows, το Linux μπορεί να προσφέρει πολλές υπηρεσίες και είναι σίγουρο ότι θα σας εντυπωσιάσει.

```
root@samba:/home/Users# ls -l
total 32
drwxrws---+ 13 3000018 users 4096 Feb  3 13:34 kafetis
drwxrws---+ 14 3000018 users 4096 Feb  3 13:27 kafetis.V2
drwxrwsr-x+  2 3000000 users 4096 Feb  3 13:19 pit
drwxrws---+ 14 3000016 users 4096 Feb  3 13:28 pit.V2
root@samba:/home/Users#
```

Για την τήρηση των δεδομένων κάθε χρήστη του domain, δημιουργούνται δύο ξεχωριστοί φάκελοι. Οι φάκελοι με το επίθεμα ".V2" διατηρούν τα δεδομένα του εκάστοτε λογαριασμού, για τα μηχανήματα που τρέχουν Windows Vista ή κάτι μεταγενέστερο.

Skill: Intermediate
Tags: TorGuard, VPN, pfSense, NAT, aliases

Στον αγώνα για ανέμελο torrenting, μέρος 3/3

Πρώτη γραμμή άμυνας, με το pfSense

Στα δύο προηγούμενα άρθρα της σειράς γνωρίσαμε την υπηρεσία του TorGuard και μετά δείξαμε πώς φτιάχνουμε το δικό μας Seedbox, με όλους τους απαραίτητους μηχανισμούς για την προστασία της ιδιωτικότητας αλλά και της ανωνυμίας μας. Στο παρόν άρθρο μετακινούμε τους εν λόγω μηχανισμούς στην πρώτη γραμμή, ώστε να μην αφορούν μεμονωμένες συσκευές αλλά ολόκληρο το τοπικό μας δίκτυο.

του Χρήστου Βαρελά

Αναλυτικότερα, θα δούμε πώς από έναν router που τρέχει pfSense (https://deltahacker.gr/?p=8234) πραγματοποιούμε δύο ή περισσότερες μόνιμες συνδέσεις προς VPN servers του TorGuard, ώστε διαφορετικά υποσύνολα συσκευών του τοπικού δικτύου να βγαίνουν στο Internet μέσω διαφορετικών απομακρυσμένων servers. Η ανωνυμία αλλά και η ιδιωτικότητα διασφαλίζονται σε κάθε περίπτωση, ωστόσο αναλόγως του βασικού ρόλου κάθε συσκευής είναι πιθανό να βγαίνει στο Internet, π.χ., μέσω Ελβετίας (Seedbox), Ισλανδίας (Linux servers) ή Αμερικής (Netflix clients).

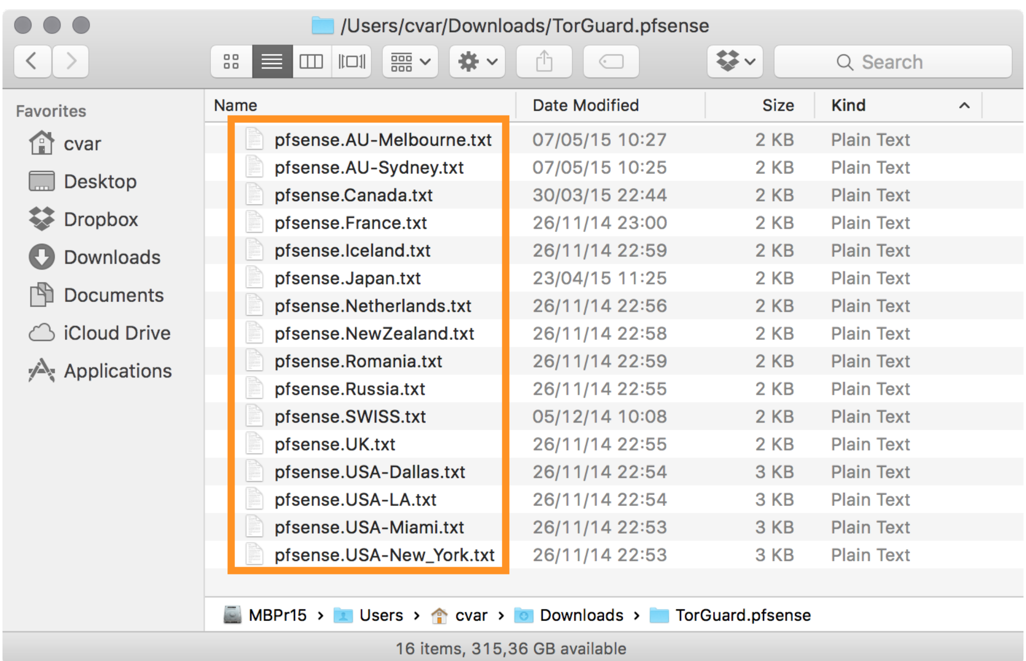
Ο router μας τρέχει το pfSense 2.2.6-RELEASE 64bit. Διαθέτει μία κάρτα δικτύου WAN, η οποία επικοινωνεί με το ADSL modem του ISP μας, καθώς και δύο άλλες κάρτες δικτύου (LAN, OPT1), οι οποίες είναι γεφυρωμένες μεταξύ τους (bridged). Τη γέφυρα (OPT2) βλέπουν όλες οι συσκευές του τοπικού δικτύου και, παρεμπιπτόντως, σε ένα από τα διαθέσιμα ports του OPT2 υπάρχει κι ένα Wireless Access Point. Σε ένα απλούστερο και πιο συνηθισμένο setup έχουμε μόνο τις κάρτες WAN και LAN. Πάντως όλα όσα ακολουθούν δεν εξαρτώνται από το πλήθος των καρτών δικτύου που διαθέτει το pfSense.

Θα εργαστούμε εξάλλου με τρόπο παρόμοιο (αλλά όχι ίδιο) μ' εκείνον που είχαμε εργαστεί όταν συνδέσαμε το pfSense με απομακρυσμένο Access Server (https://deltahacker.gr/?p=15109), σε VPS της DigitalOcean (https://deltahacker.gr/?p=15064).

Υπόδειξη. Αν δεν έχετε διαβάσει τα δύο προαναφερθέντα άρθρα, μην το κάνετε τώρα: Αυτή τη φορά δεν υπάρχει Access Server, ενώ και οι συνδέσεις VPN προς τους servers του TorGuard δεν επιτυγχάνονται με τον ίδιο τρόπο που επιτυγχάνεται η σύνδεση προς τον Access Server.

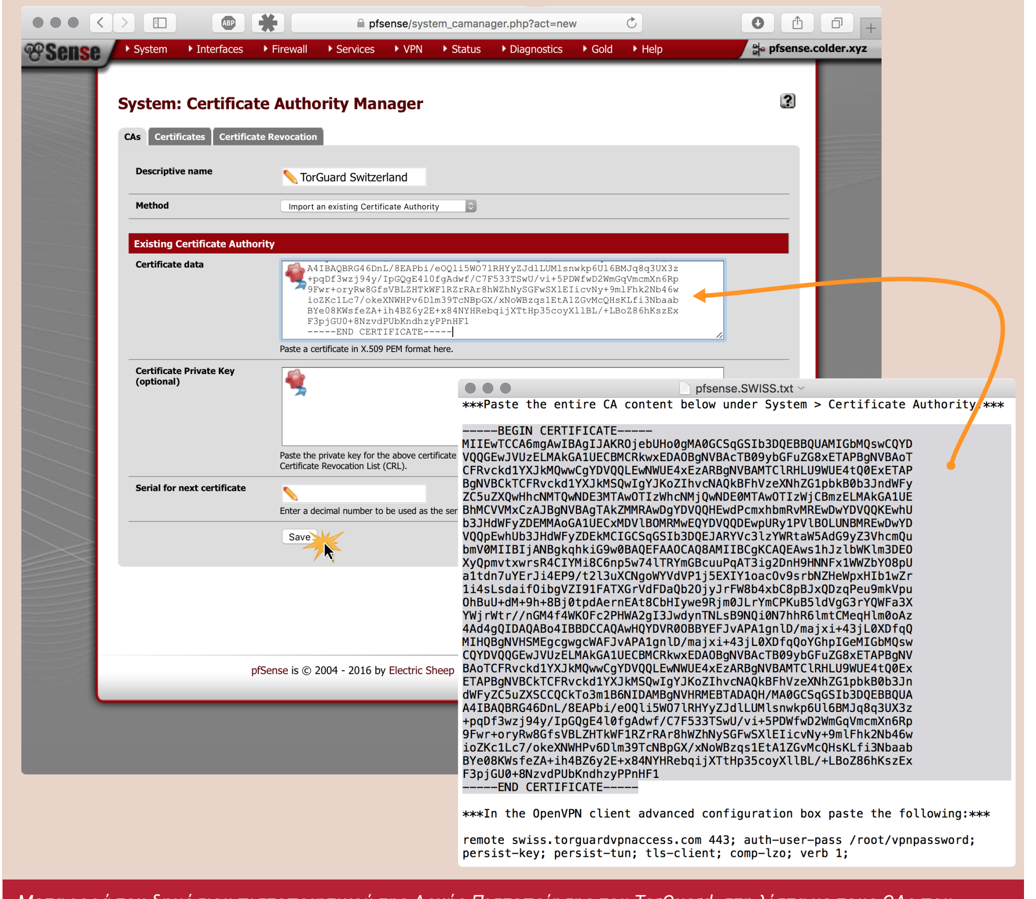
Για τη συνέχεια, υποθέτουμε ότι έχετε ήδη ενεργό λογαριασμό για την υπηρεσία Anonymous VPS του TorGuard (https://torguard.net/aff.php?aff=1790). Χωρίς άλλες περιστροφές, ας πιάσουμε δουλειά.

Βήμα 1, λήψη αρχείου με configurations. Πρόκειται για ένα μικρό ZIP το οποίο λαμβάνουμε από το http://torguard.net/downloads/TorGuard.pfsense.zip. Αποσυμπιέζοντάς το βλέπουμε ότι περιλαμβάνει 16 στο πλήθος text files – ή τουλάχιστον αυτό ίσχυε με το ZIP που εμείς κατεβάσαμε. Καθένα από τα text files αντιστοιχεί σε διαφορετικό TorGuard VPN server, σε διαφορετική γεωγραφική περιοχή στον πλανήτη. Με μια ματιά στα ονόματα των αρχείων φαίνεται αμέσως για ποιες γεωγραφικές περιοχές μιλάμε. Θα ξεκινήσουμε με το αρχείο pfsense.SWISS.txt, ώστε να συνδέσουμε το pfSense box με VPN server του TorGuard στην Ελβετία. Λίγο αργότερα, θα κάνουμε ό,τι χρειάζεται ώστε το Seedbox που έχουμε να βγαίνει στο Internet μέσω του εν λόγω TorGuard server.

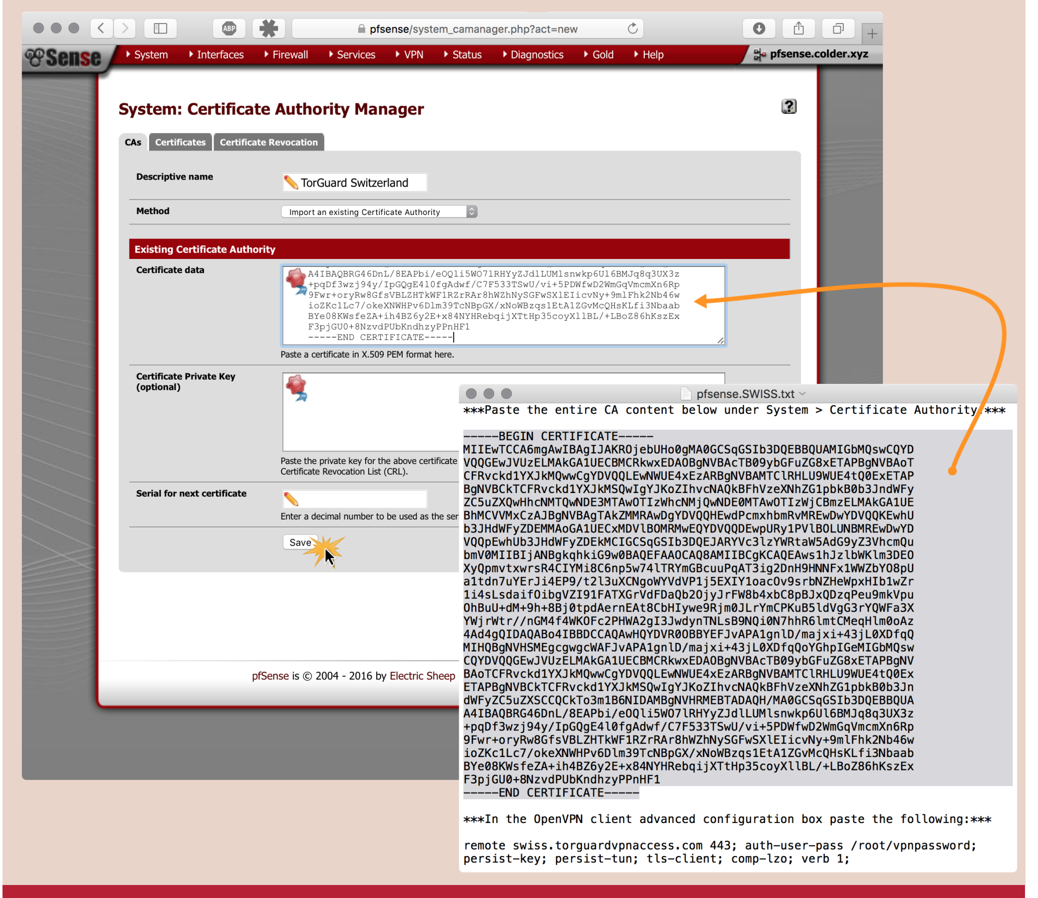


Καθένα από τα 16 αρχεία κειμένου περιλαμβάνει το δημόσιο πιστοποιητικό που χρησιμοποιεί η Αρχή Πιστοποίησης του TorGuard, καθώς και οδηγίες για τη σύνδεση του pfSense σε VPN server της αντίστοιχης γεωγραφικής περιοχής.

Βήμα 2, εισαγωγή δημόσιου πιστοποιητικού του TorGuard, στο pfSense. Από τον web browser της προτίμησής μας περιηγούμαστε στο web panel του pfSense, κάνουμε login στο λογαριασμό του διαχειριστή κι ακολουθούμε τη διαδρομή System → Cert Manager → CAs. Με κλικ στο εικονίδιο [+] φορτώνει μια σελίδα για την εισαγωγή ενός νέου δημόσιου πιστοποιητικού. Στο πεδίο Descriptive name, στο πάνω μέρος της σελίδας, πληκτρολογούμε κάτι περιγραφικό για το νέο πιστοποιητικό (π.χ., "TorGuard Switzerland", χωρίς τα εισαγωγικά). Θέτουμε Method = Import an existing Certificate Authority και στο πεδίο Certificate data, από κάτω, με copy και paste μεταφέρουμε το πιστοποιητικό από το αρχείο pfsense.SWISS.txt. Συγκεκριμένα, αντιγράφουμε κι επικολλούμε όλο το κείμενο μεταξύ των -----BEGIN CERTIFICATE----- και -----END CERTIFICATE---- (αυτών συμπεριλαμβανομένων). Επικυρώνουμε τη μεταφορά με ένα κλικ στο κουμπί Save, στο κάτω μέρος της σελίδας.



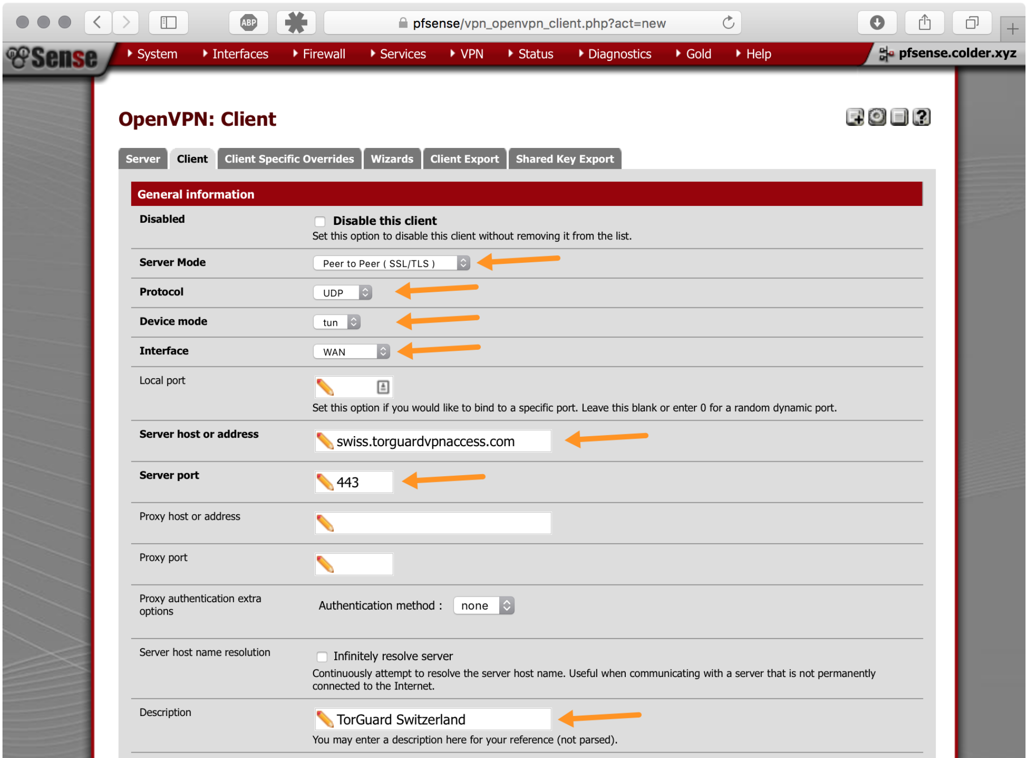
Μεταφορά του δημόσιου πιστοποιητικού της Αρχής Πιστοποίησης του TorGuard, στη λίστα με τους CAs που γνωρίζει το pfSense μας.



Ιδού τα δύο πιστοποιητικά που διαθέτει το pfSense μας έως τώρα. Το πρώτο ανήκει στον OpenVPN server του ίδιου του router (https://deltahacker.gr/?p=12109), ενώ το δεύτερο είναι εκείνο του TorGuard (πρόκειται για εκείνο που μόλις εισαγάγαμε).

Βήμα 3, ρύθμιση OpenVPN client προς τον VPN server του TorGuard. Δίνουμε VPN → OpenVPN → Client και κάνουμε κλικ πάνω στο κουμπί [+], δεξιά. Παρουσιάζεται τότε μια σελίδα για τη ρύθμιση ενός νέου OpenVPN client. Φροντίζουμε ώστε να ισχύουν τα ακόλουθα:

- **Server Mode** = Peer to Peer (SSL/TLS)
- **Protocol** = UDP
- **Device mode** = tun
- **Interface** = WAN
- **Server host or address** = swiss.torguardvpnaccess.com (η διεύθυνση αναφέρεται στο αρχειάκι pfsense.SWISS.txt)
- **Server port** = 443 (το port αναφέρεται στο pfsense.SWISS.txt)
- **Description** = TorGuard Switzerland (μπορείτε φυσικά να δώσετε όποια περιγραφή θέλετε)



Οι πρώτες γενικές ρυθμίσεις του OpenVPN client για τον TorGuard VPN server στην Ελβετία.

Συνεχίζουμε στην ίδια σελίδα και συγκεκριμένα στην ενότητα User Authentication Settings. Εκεί, στις θυρίδες Username και Password πληκτρολογούμε τα credentials του λογαριασμού μας στο TorGuard, για την υπηρεσία του Anonymous VPN.

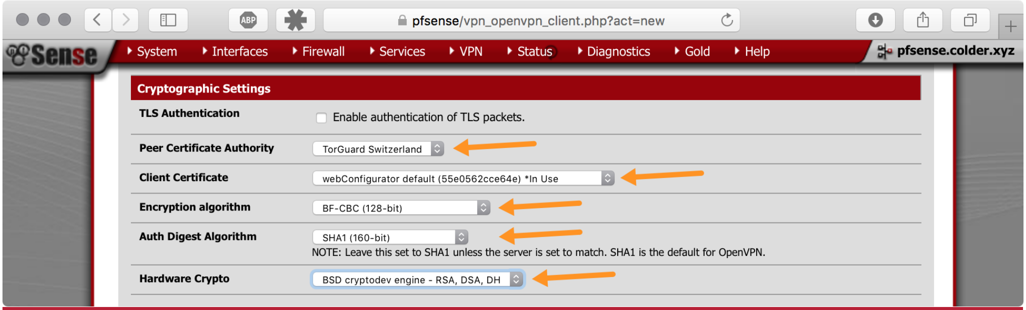


Εισαγωγή των στοιχείων του λογαριασμού μας στο TorGuard, για την υπηρεσία Anonymous VPN.

Αμέσως από κάτω, στην ενότητα Cryptographic Settings, βεβαιωνόμαστε για τα ακόλουθα:

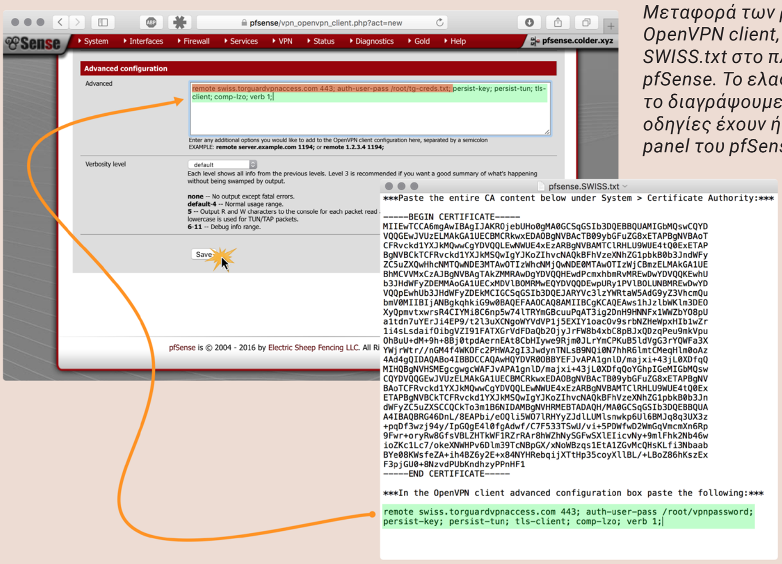
- το **TLS Authentication** να *μην* είναι τσεκαρισμένο
- **Peer Certificate Authority** = TorGuard Switzerland (ή όπως αλλιώς ονομάσαμε το δημόσιο πιστοποιητικό που εισαγάγαμε στο βήμα 1)

- **Client Certificate** = webConfigurator default (...) *In Use
- **Encryption algorithm** = BF-CBC (128-bit)
- **Auth Digest Algorithm** = SHA1 (160-bit)
- **Hardware Crypto** = BSD cryptodev engine - RSA, DSA, DH



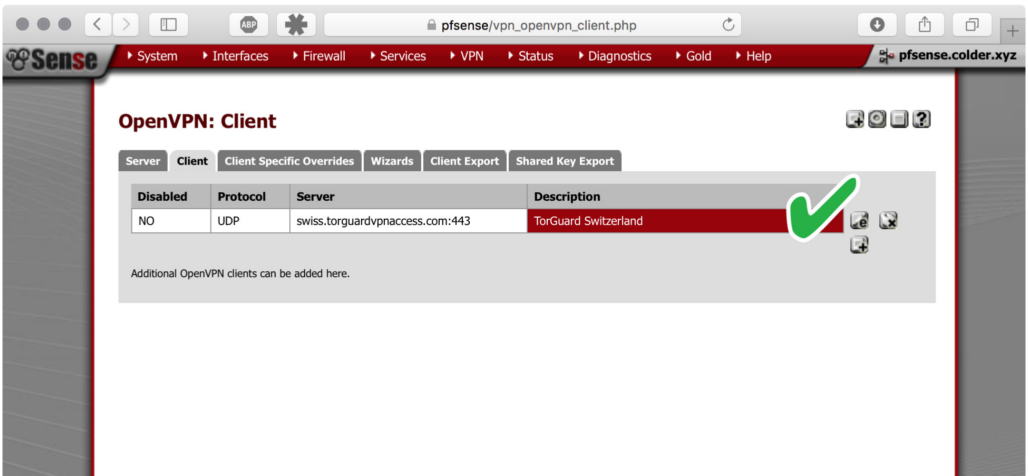
Οι ρυθμίσεις του νέου OpenVPN client, οι οποίες αφορούν στην κρυπτογράφηση. Για το Peer Certificate Authority θα επιλέξετε το πιστοποιητικό που εισαγάγατε στο βήμα 1.

Στην ίδια σελίδα του pfSense αλλά πιο κάτω, υπάρχει η ενότητα Advanced configuration. Ανοίγουμε το αρχείο pfsense.SWISS.txt κι αντιγράφουμε τις οδηγίες για τον OpenVPN client που υπάρχουν στο τέλος του αρχείου. Τις επικολλούμε στο πλαίσιο ονόματι Advanced του pfSense κι αμέσως μετά διαγράφουμε το τμήμα "remote swiss.torguardvpnaccess.com 443; auth-user-pass /root/vpnpassword;". Τώρα, όλες τις ρυθμίσεις και τις επεμβάσεις που μόλις κάναμε σ' αυτό το βήμα, το υπ' αριθμόν 3, τις επικυρώνουμε με κλικ στο κουμπί Save.

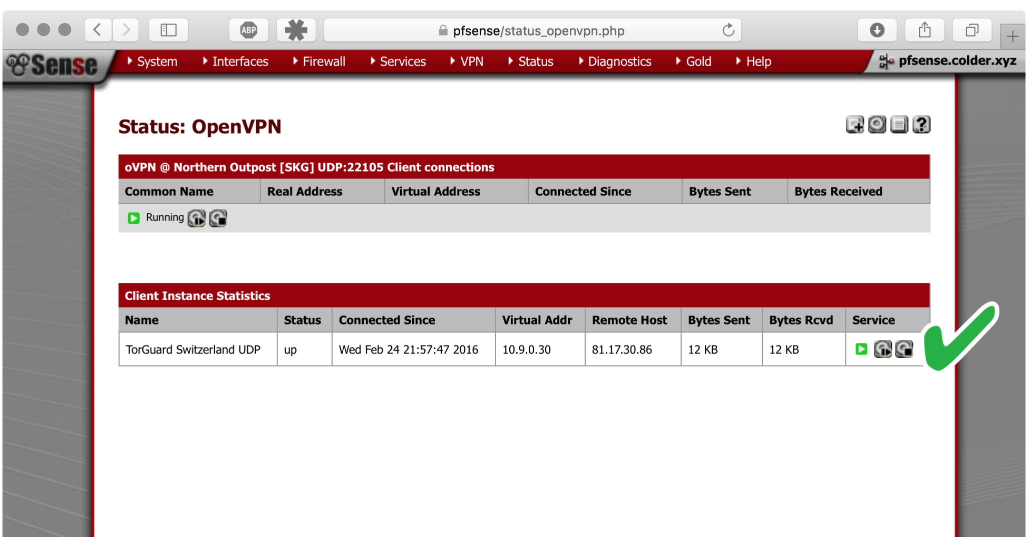


Μεταφορά των ρυθμίσεων για τον OpenVPN client, από το αρχείο pfsense.SWISS.txt στο πλαίσιο Advanced του pfSense. Το ελαφρώς κόκκινο τμήμα θα το διαγράφουμε, αφού οι αντίστοιχες οδηγίες έχουν ήδη εισαχθεί από το web panel του pfSense.

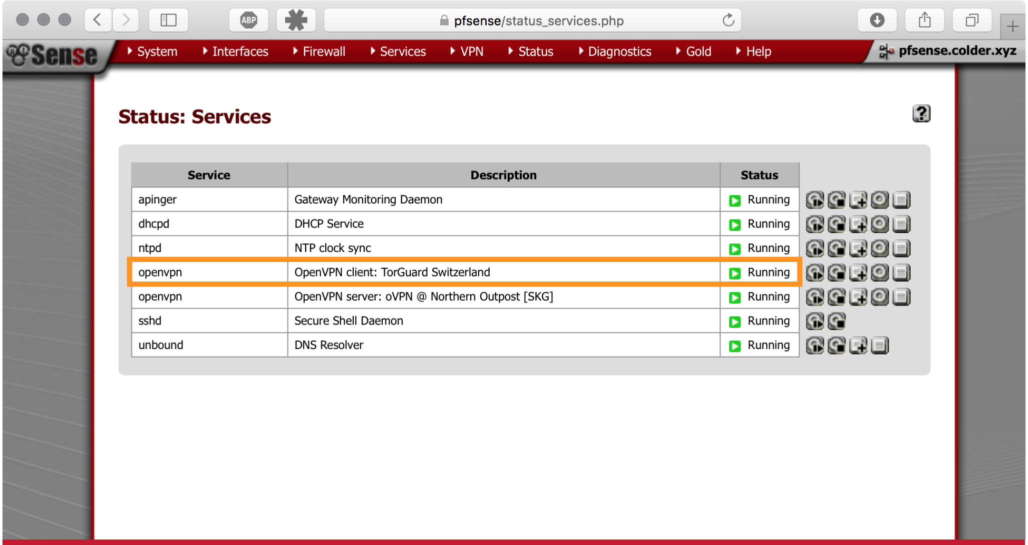
Αν όλα έχουν πάει καλά τότε ο OpenVPN client του pfSense θα συνδεθεί στον TorGuard VPN server στην Ελβετία. Χρειάζεται όμως κι άλλη δουλειά, πριν μία ή περισσότερες συσκευές πίσω από το pfSense αρχίσουν να βγαίνουν στο Internet μέσω Ελβετίας. Προς το παρόν, ας κάνουμε ένα σύντομο διάλειμμα κι ας δούμε τι έχει να πει το pfSense για το νέο κρυπτογραφημένο τούνελ που έχει δημιουργηθεί. Δείτε τα τρία screenshots που ακολουθούν.



Από το VPN → OpenVPN → Client είναι φανερό ότι ο νέος client είναι ενεργός (Disabled = NO). Έχει όμως επιτευχθεί και σύνδεση;

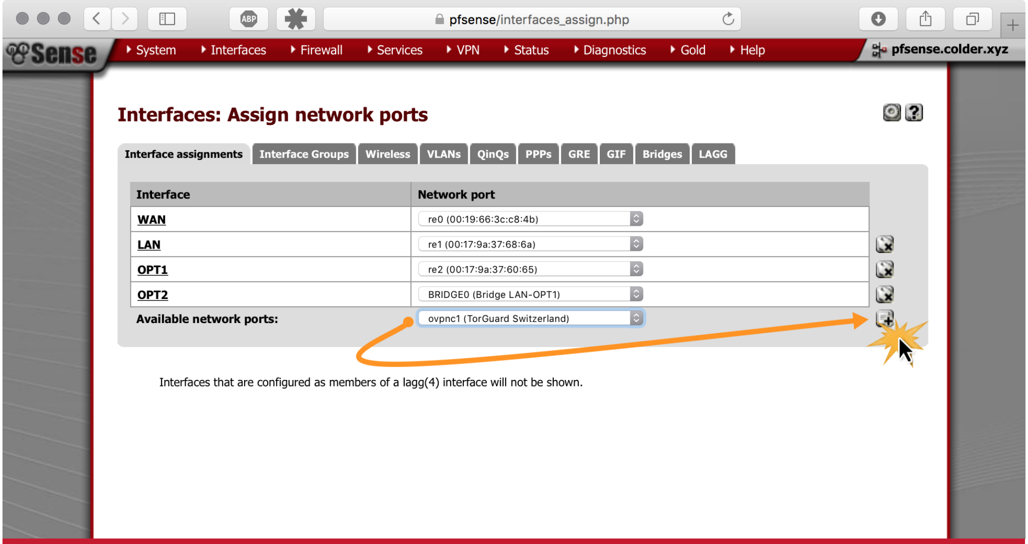


Δίνοντας Status → OpenVPN διαπιστώνουμε ότι υπάρχει ένα ενεργό OpenVPN client instance (Status = up), το οποίο αφορά στον client που μόλις ορίσαμε (Name = TorGuard Switzerland UDP). Διακρίνονται το δημόσιο IP του απομακρυσμένου OpenVPN server καθώς και το IP που έχει αντιστοιχιστεί στο tun0 interface, μέσω του οποίου υλοποιείται το κρυπτογραφημένο τούνελ μεταξύ του pfSense και του TorGuard VPN server.

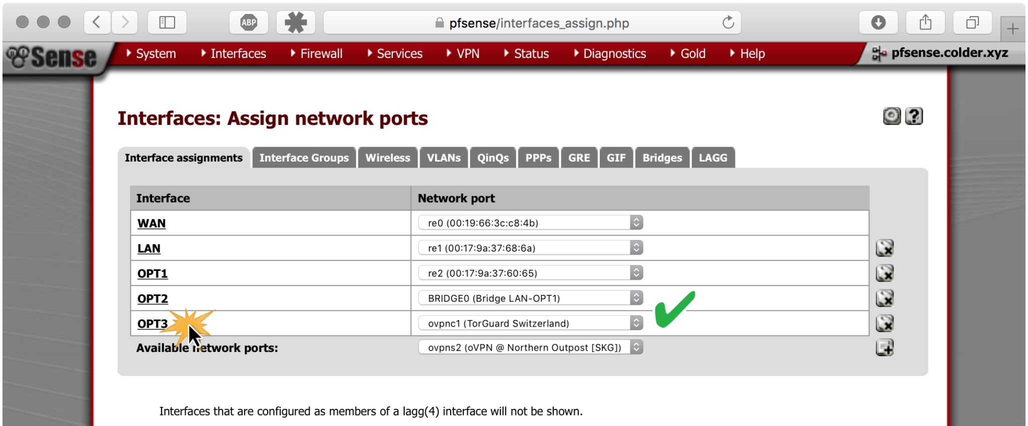


Ένας τελευταίος έλεγχος, πριν πιάσουμε ξανά δουλειά (Status → Services): O OpenVPN client του "TorGuard Switzerland" τρέχει (Running) – κι αυτό είναι καλό.

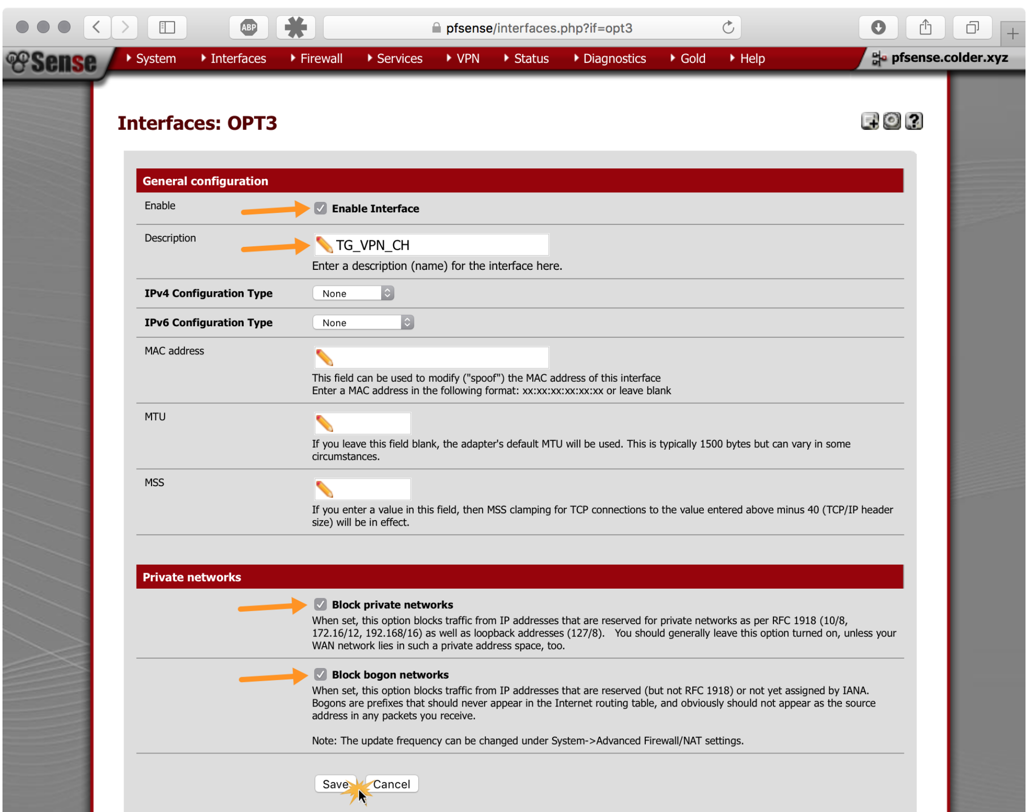
Βήμα 4, δημιουργία νέου network interface για τη νέα σύνδεση VPN. Χρειαζόμαστε νέους κανόνες για το NAT αλλά και για το firewall του router μας. Προς τούτο, θα ορίσουμε ένα νέο network interface για τη σύνδεση στον απομακρυσμένο TorGuard VPN server. Δείτε τα screenshots που ακολουθούν και διαβάστε τις αντίστοιχες περιγραφές.



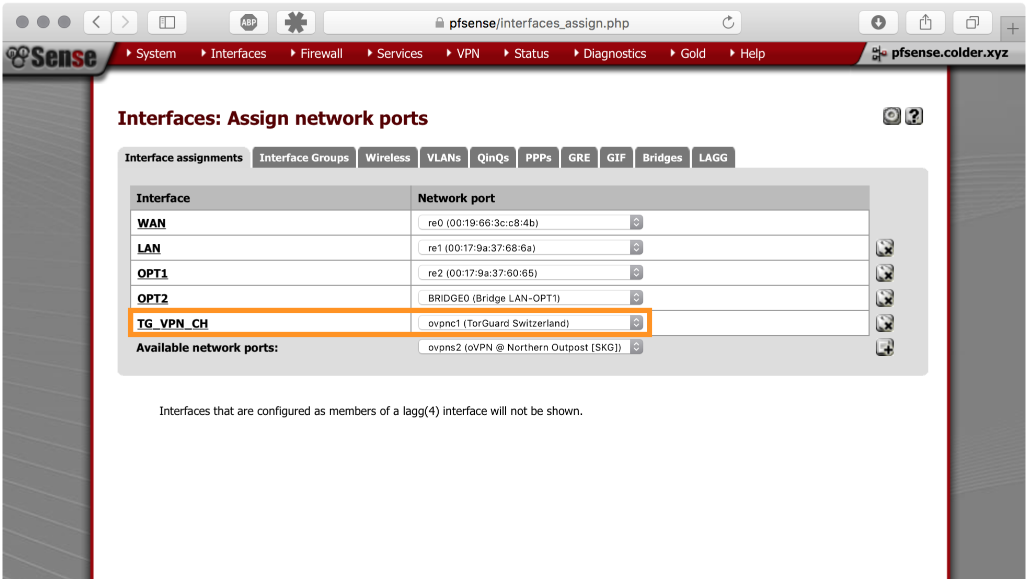
Ξεκινάμε επιλέγοντας Interfaces → (assign). Για το Available network ports επιλέγουμε το ovpnc1 (TorGuard Switzerland). Τα ονόματα ενδέχεται να διαφέρουν για το setup σας, φροντίστε ωστόσο να διαλέξετε το network port που αντιστοιχεί στη σύνδεση προς τον TorGuard VPN server. Στα δεξιά, κάντε ένα κλικ στο [+].



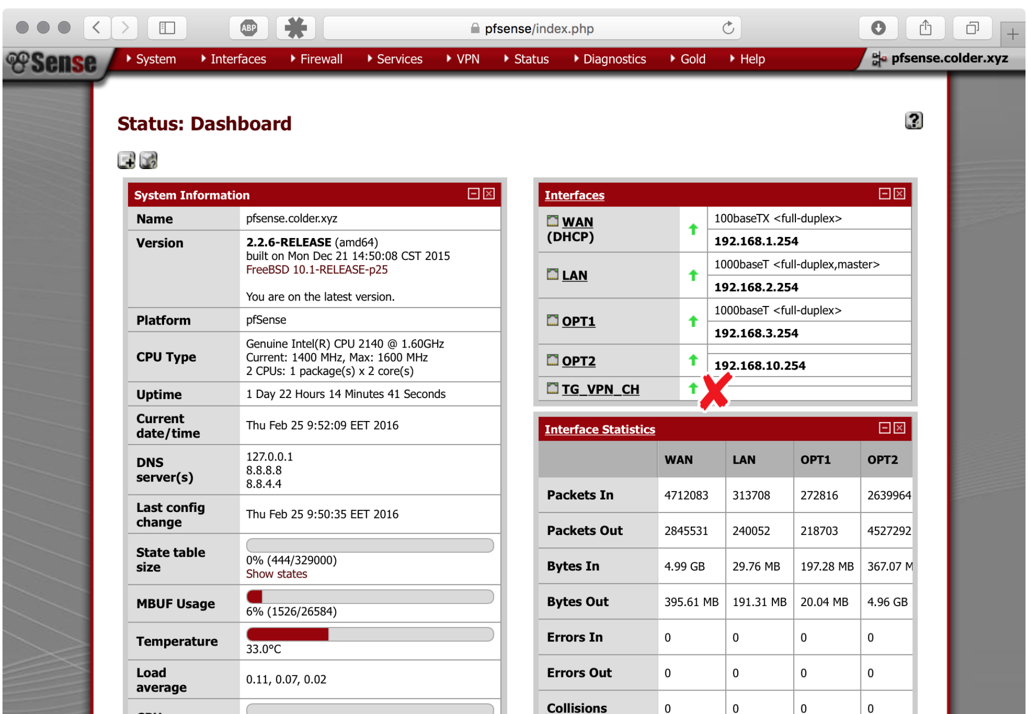
Όπως βλέπετε στο παράδειγμά μας, έχουμε πλέον ένα νέο network interface, το OPT3. Σε ένα απλούστερο setup, όπου υπάρχουν μόνο τα interfaces WAN και LAN, το νέο interface θα ονομάζεται OPT1. Κάνουμε κλικ πάνω στ' όνομά του.



Φροντίζουμε ώστε το Enable Interface να είναι τσεκαρισμένο, και στη θυρίδα Description πληκτρολογούμε ένα πιο περιγραφικό όνομα για το interface (π.χ., TG_VPN_CH, όπου το "CH" είναι ο κωδικός δύο γραμμάτων της Ελβετίας). Πριν παγιώσουμε την αλλαγή, μ' άλλα λόγια πριν ενεργοποιήσουμε το νέο interface, τσεκάρουμε τα Block private networks και Block bogon networks.

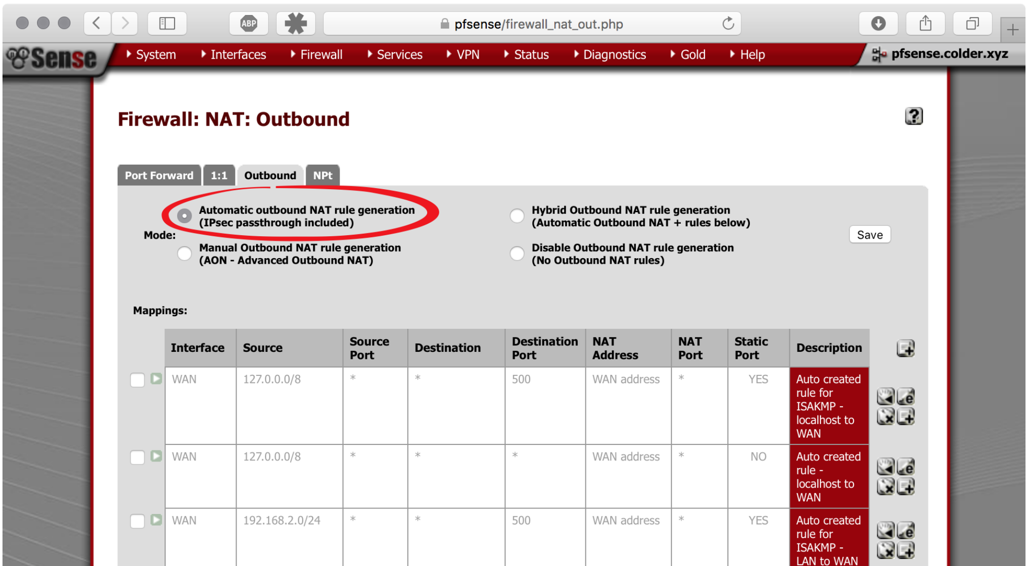


Ιδού το νέο network interface, με το νέο του, φιλικό όνομα. Υπενθυμίζουμε ότι αντιστοιχεί στη σύνδεσή μας προς τον VPN server στην Ελβετία.

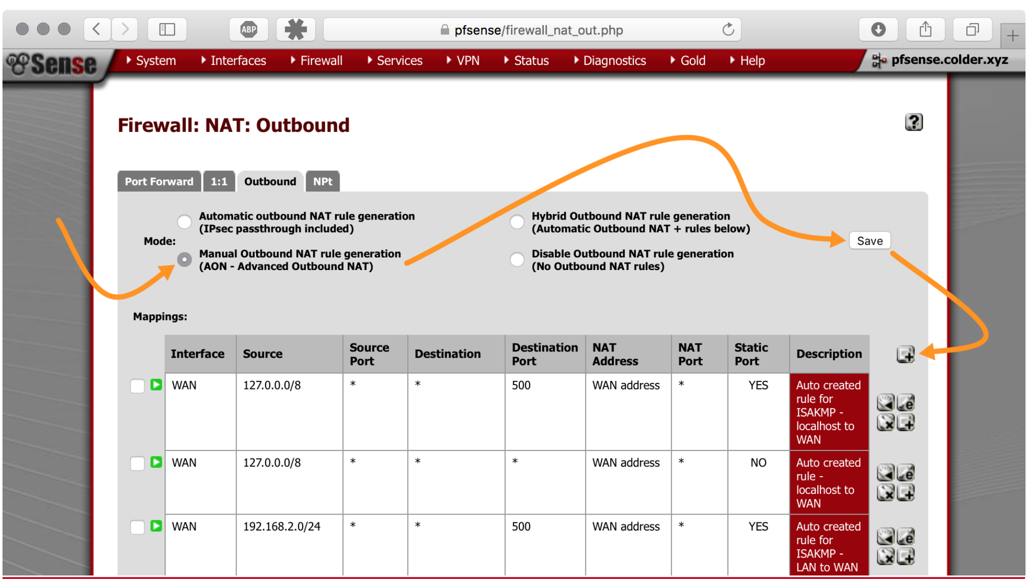


Όπως βλέπουμε στην ενότητα Interfaces της σελίδας Status → Dashboard, στο νέο interface δεν έχει ακόμα αντιστοιχιστεί διεύθυνση IP. Σε λίγο θ' αλλάξει αυτό, πρώτα όμως έχουμε να φροντίσουμε για το NAT.

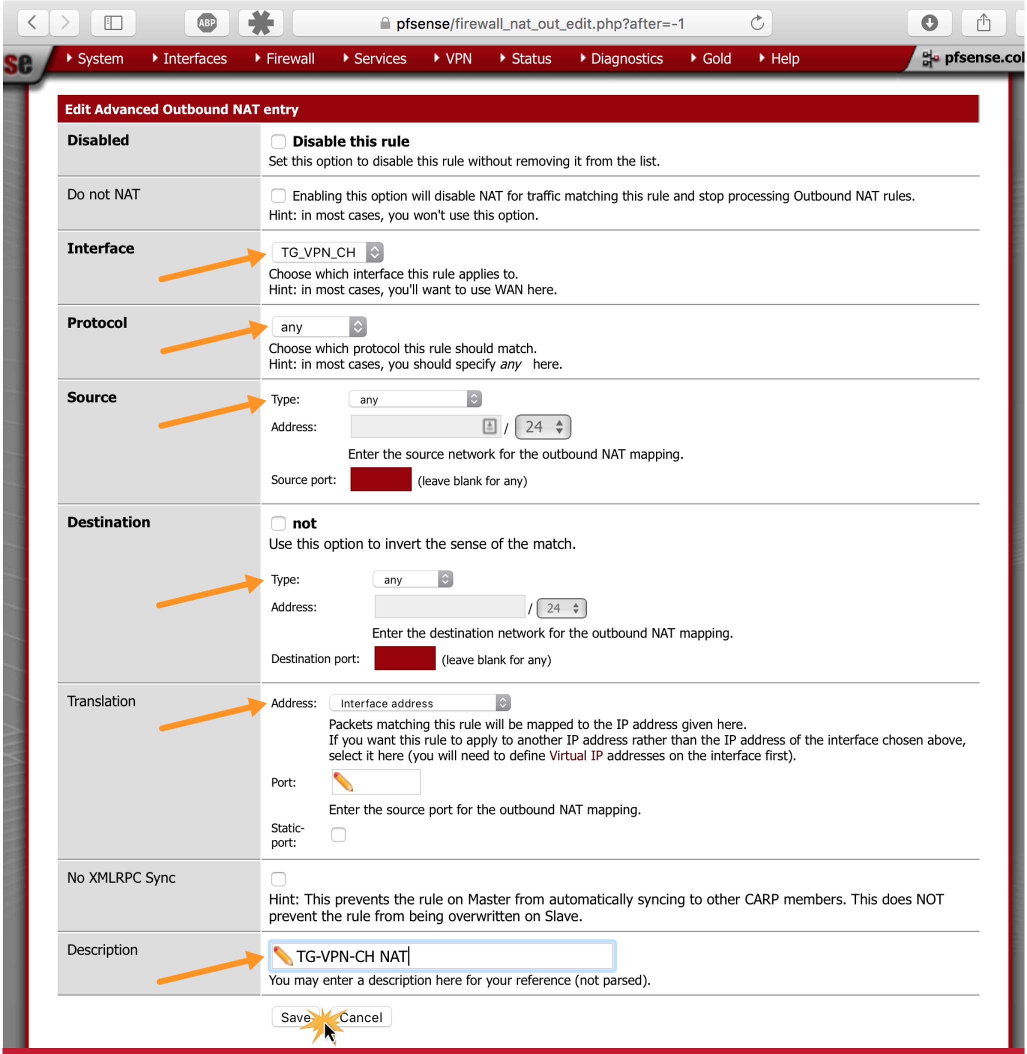
Βήμα 5, επέμβαση στους κανόνες για το NAT. Για τους νέους κανόνες NAT ακολουθούμε τη διαδρομή Firewall → NAT → Outbound. Όπως βλέπετε, προεπιλεγμένο είναι το Automatic outbound NAT rule generation (IPsec passthrough included).



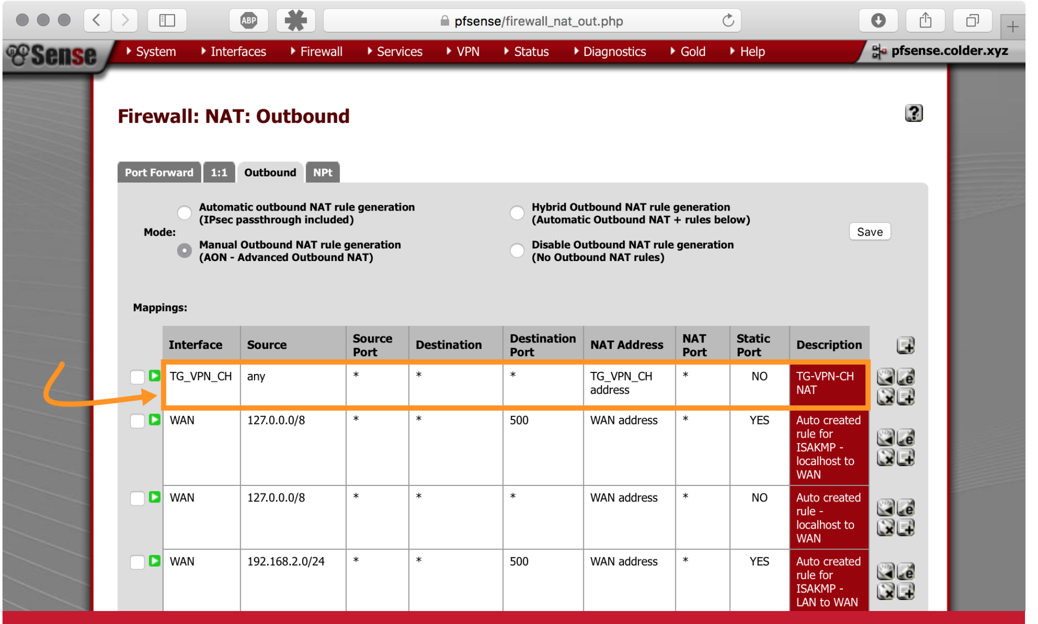
Εξ ορισμού, οι κανόνες NAT (Network Address Translation) δημιουργούνται αυτόματα στο pfSense κι αφορούν στη διεύθυνση IP του WAN interface.



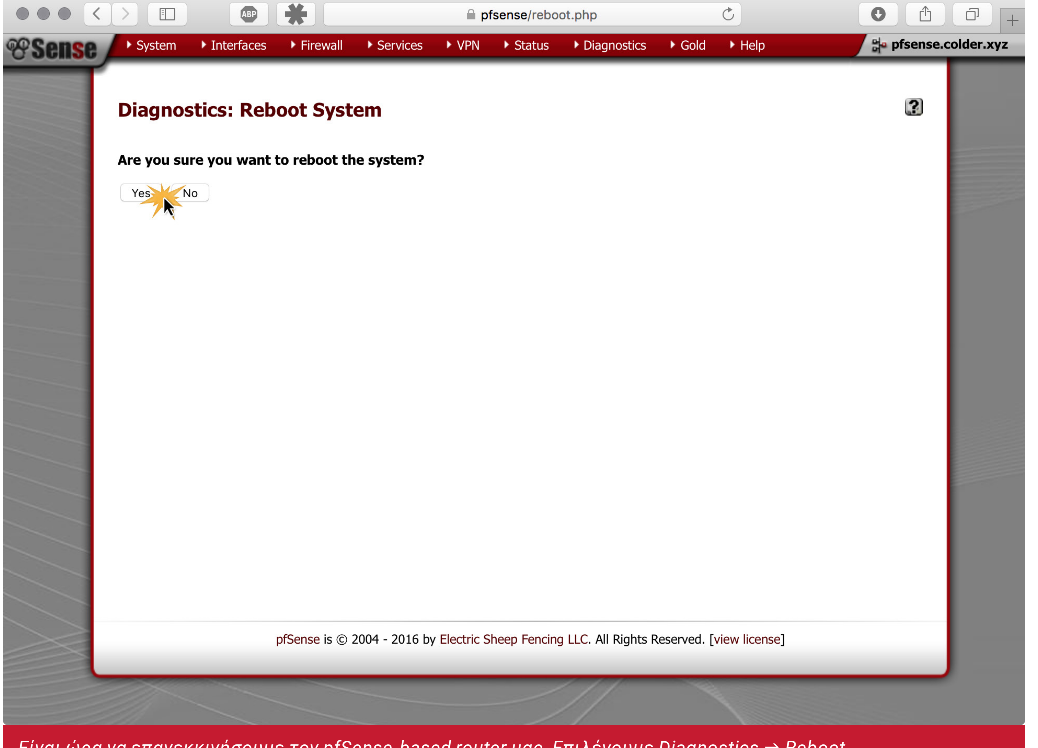
*Θέλουμε να ορίσουμε έναν κανόνα NAT *και* για το TG_VPN_CH interface, οπότε επιλέγουμε το Manual Outbound NAT rule generation (AON - Advanced Outbound NAT), μετά κάνουμε ένα κλικ στο κουμπί Save κι αμέσως μετά άλλο ένα στο κουμπάκι [+], πάνω δεξιά, ώστε να ορίσουμε τον κανόνα μας.*



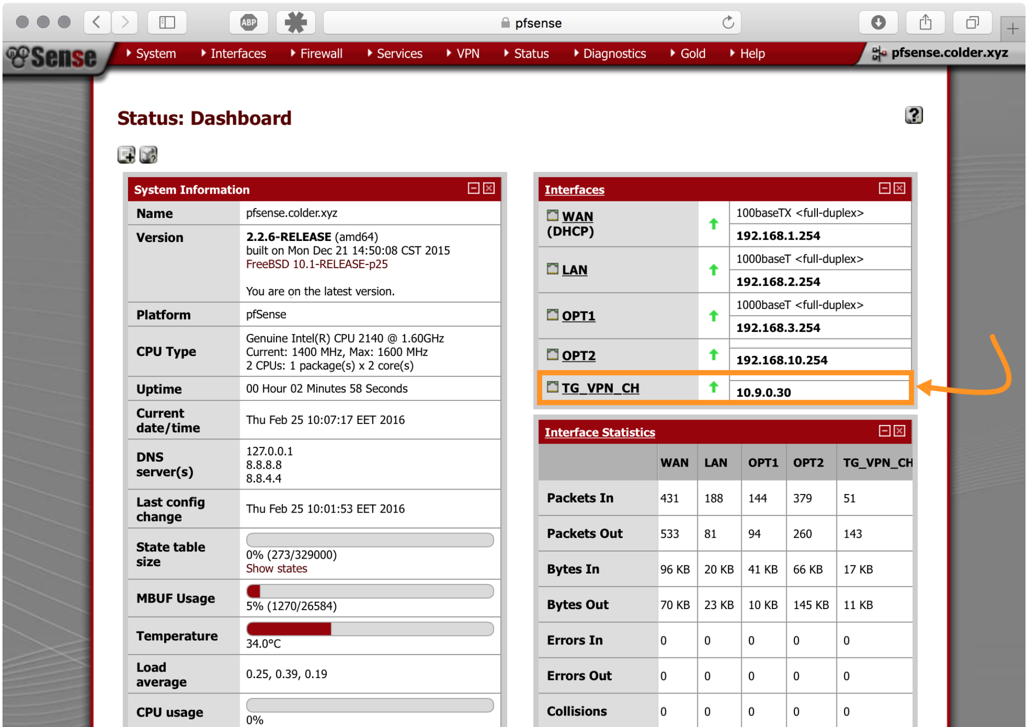
Στη σελίδα για τον ορισμό του κανόνα NAT, αρχικά ξεκαθαρίζουμε ότι αφορά στο TG_VPN_CH interface. Για τα Protocol, Source και Destination ορίζουμε το any, ενώ στην περιοχή Translation φροντίζουμε ώστε να ισχύει Address = Interface address. Τέλος, στη θυρίδα ονόματι Description πληκτρολογούμε μια χαρακτηριστική περιγραφή για τον κανόνα και μετά πατάμε στο κουμπί Save, από κάτω.



Ιδού ο νέος κανόνας NAT, για το network interface της σύνδεσης προς τον Ελβετικό TorGuard VPN server.



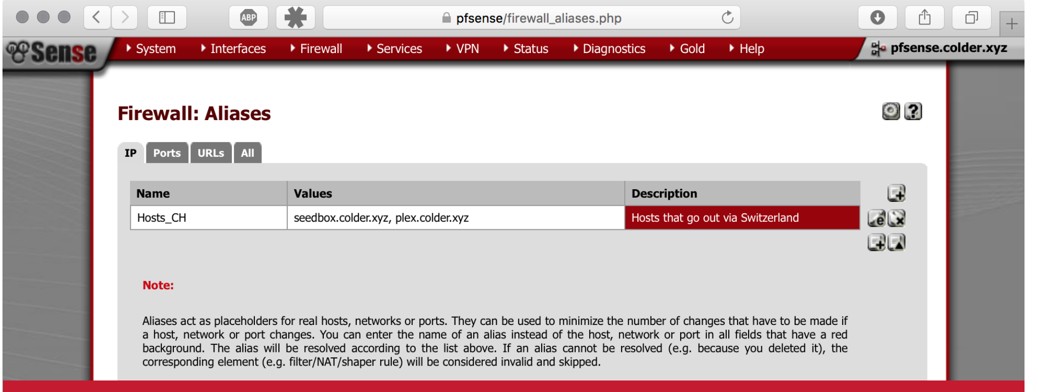
Είναι ώρα να επανεκκινήσουμε τον pfSense-based router μας. Επιλέγουμε Diagnostics → Reboot.



Μόλις ο router επανεκκινήσει, συνδεόμαστε στο web panel του pfSense και δίνουμε Status → Dashboard. Παρατηρήστε την ενότητα Interfaces: το TG_VPN_CH είναι ενεργό και μάλιστα του έχει αντιστοιχιστεί διεύθυνση IP.

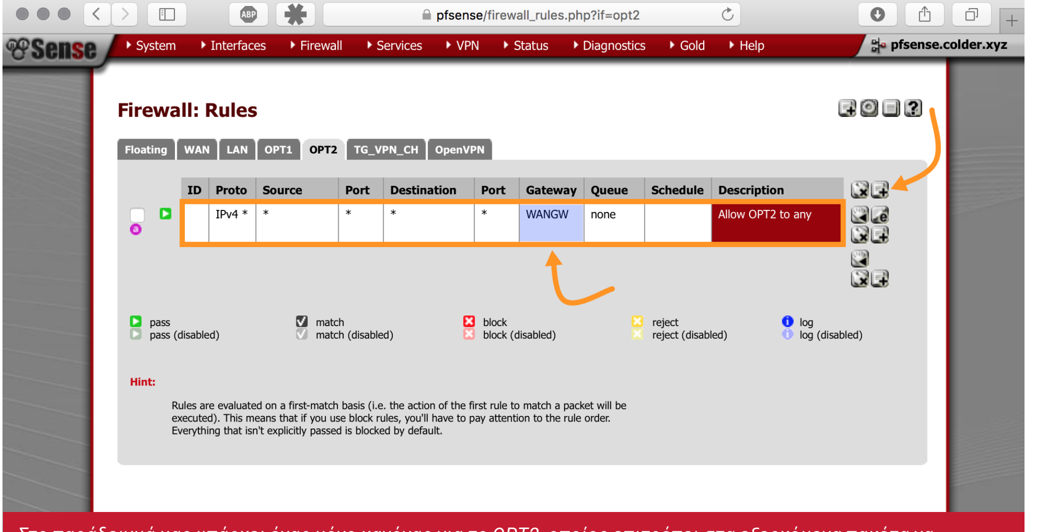
Βήμα 6, δημιουργία alias. Δεν θέλουμε να βγαίνουν όλες οι συσκευές του τοπικού μας δικτύου στο Internet μέσω του Ελβετικού VPN server, παρά μόνον όσες έχουμε εμείς υποδείξει. Στο pfSense, ένας καλός τρόπος για να καθορίζουμε συσκευές στις οποίες θέλουμε ν' αναφερόμαστε συνολικά κι όχι μεμονωμένα, είναι με χρήση των aliases. Περισσότερα γι' αυτά μπορείτε να διαβάσετε στο https://deltahacker.gr/?p=15323 – και συγκεκριμένα στην παράγραφο "Τα aliases του pfSense". Στο πλαίσιο των πειραματισμών μας φτιάξαμε το alias ονόματι Hosts_CH, το οποίο περιλαμβάνει τις εσωτερικές διευθύνσεις IP δύο VMs που θέλουμε να βγαίνουν στο Internet μέσω του Ελβετικού VPN server. Το ένα VM λειτουργεί ως Plex media server (https://deltahacker.gr/?p=15549) ενώ το άλλο είναι το Seedbox μας, με το Transmission (https://deltahacker.gr/?p=15791). Για το Seedbox δείτε το δεύτερο άρθρο της σειράς μας.

Σημείωση. Αν πρόκειται να ρυθμίσετε τον pfSense-based router σας ώστε να λειτουργεί ως TorGuard VPN client, τότε εφαρμόζοντας όσα περιγράφονται στο άρθρο για το Seedbox σταματήστε αμέσως μετά τη ρύθμιση του Transmission. Μην προχωρήσετε, δηλαδή, στη λειτουργικότητα OpenVPN client, ενώ και το ruleset του iptables αφήστε το ως έχει.

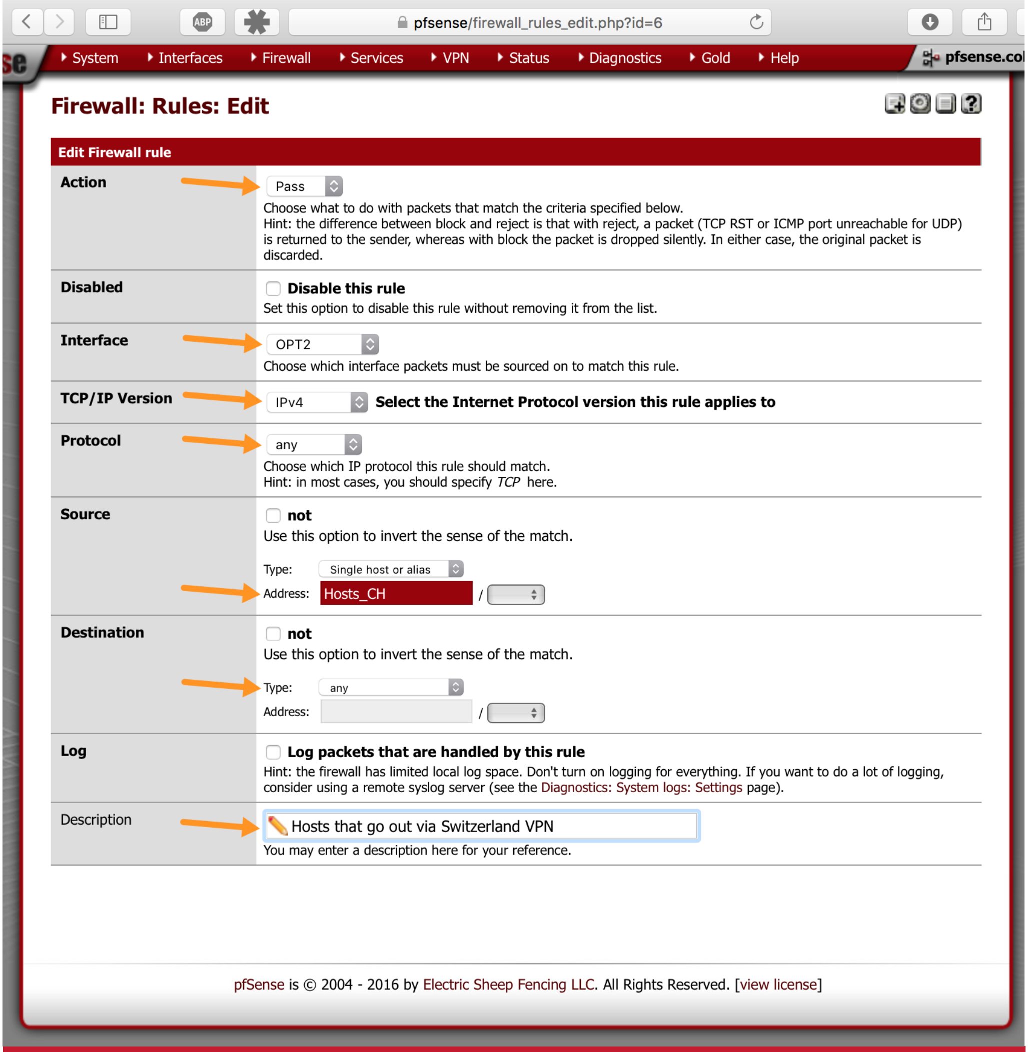


Το alias ονόματι Hosts_CH περιλαμβάνει τις εσωτερικές διευθύνσεις IP δύο VMs που θέλουμε να βγαίνουν στο Internet μέσω του Ελβετικού VPN server. Το ένα VM λειτουργεί ως Plex media server ενώ το άλλο είναι το Seedbox μας, με το Transmission.

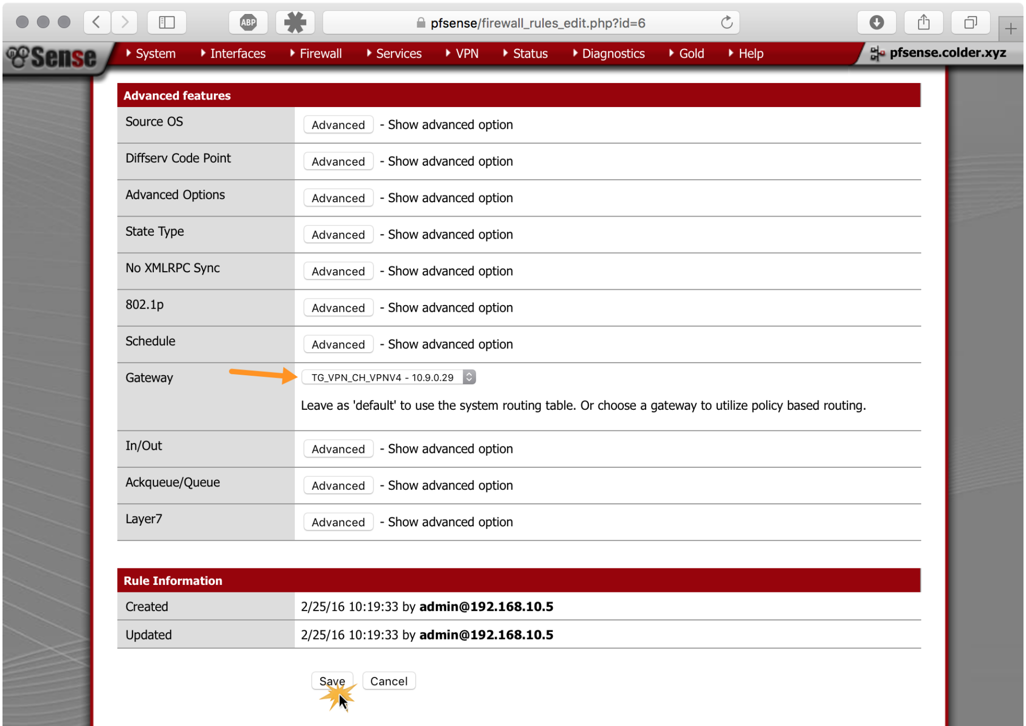
Βήμα 7, κανόνες για το firewall. Το ότι φτιάξαμε ένα alias με τα hosts που θέλουμε να βγαίνουν στο Internet μέσω του Ελβετικού TorGuard VPN, δεν σημαίνει ότι πράγματι βγαίνουν έξω μέσω του συγκεκριμένου server. Χρειαζόμαστε κι έναν κατάλληλο κανόνα στο ruleset του pfSense. Ξεκινάμε, λοιπόν, επιλέγοντας Firewall → Rules. Το network interface για το οποίο θέλουμε να ορίσουμε νέο κανόνα είναι το LAN ή, τέλος πάντων, εκείνο που βλέπουν οι συσκευές πίσω από τον router. Στο δικό μας setup, αντί για το LAN οι συσκευές βλέπουν το OPT2 (bridge των LAN, OPT1).



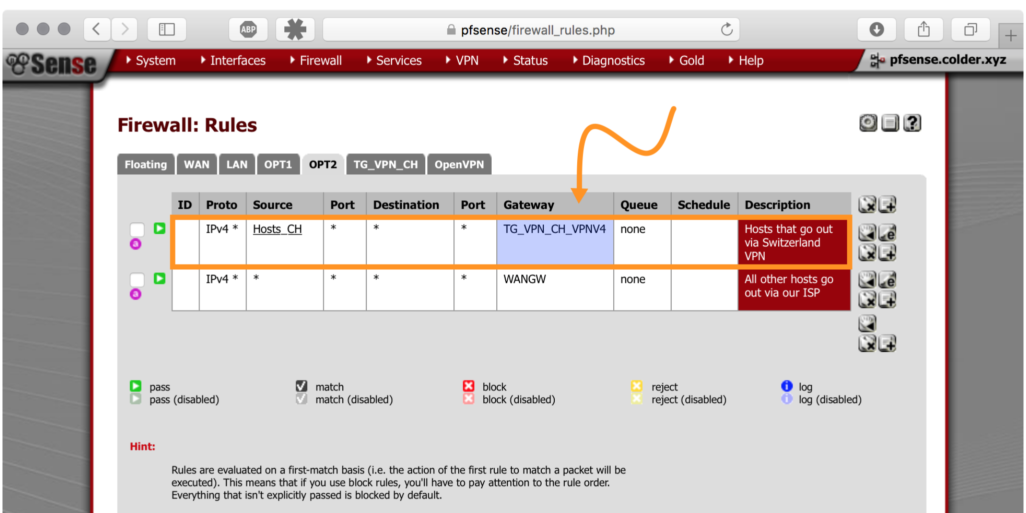
Στο παράδειγμά μας υπάρχει ένας μόνο κανόνας για το OPT2, οποίος επιτρέπει στα εξερχόμενα πακέτα να βγαίνουν έξω μέσω του gateway για το WAN interface. Για την ακρίβεια, ο κανόνας αρχικά επέτρεπε στα πακέτα να βγαίνουν έξω μέσω του προκαθορισμένου gateway, όμως τον τροποποιήσαμε ελαφρώς ώστε ο gateway να καθορίζεται ρητά. Αυτό το κάναμε διότι μετά την προσθήκη του νέου κανόνα (ή γενικότερα των νέων κανόνων) που θα γίνει σε πολύ λίγο, ο παρών κανόνας θα εφαρμόζεται μόνον όταν οι προηγούμενοι δεν ταιριάζουν. Διαφορετικά: Όταν ένα εξερχόμενο πακέτο προέρχεται από συσκευή που δεν προβλέπεται να βγαίνει στο Internet μέσω TorGuard VPN server, τότε και μόνο τότε θα εξέρχεται μέσω του ISP μας. Προκειμένου να προσθέσουμε νέο κανόνα πάνω από τον προϋπάρχοντα, πάνω δεξιά κάνουμε ένα κλικ στο κουμπάκι [+].



Εδώ βλέπουμε τη σελίδα προσθήκης νέου κανόνα. Φροντίστε ώστε και για τον δικό σας να ισχύουν όσα υποδεικνύονται από τα βελάκια. Ενδιαφέρον παρουσιάζει η τιμή που έχουμε δώσει στο Source. Για το Type επιλέξαμε το Single host or alias και στο πεδίο Address, από κάτω, πληκτρολογήσαμε το όνομα του Alias που ορίσαμε προηγουμένως. Λέμε, μ' άλλα λόγια, ότι ο κανόνας αφορά σε εξερχόμενα πακέτα τα οποία προέρχονται από συσκευές της λίστας Hosts_CH.

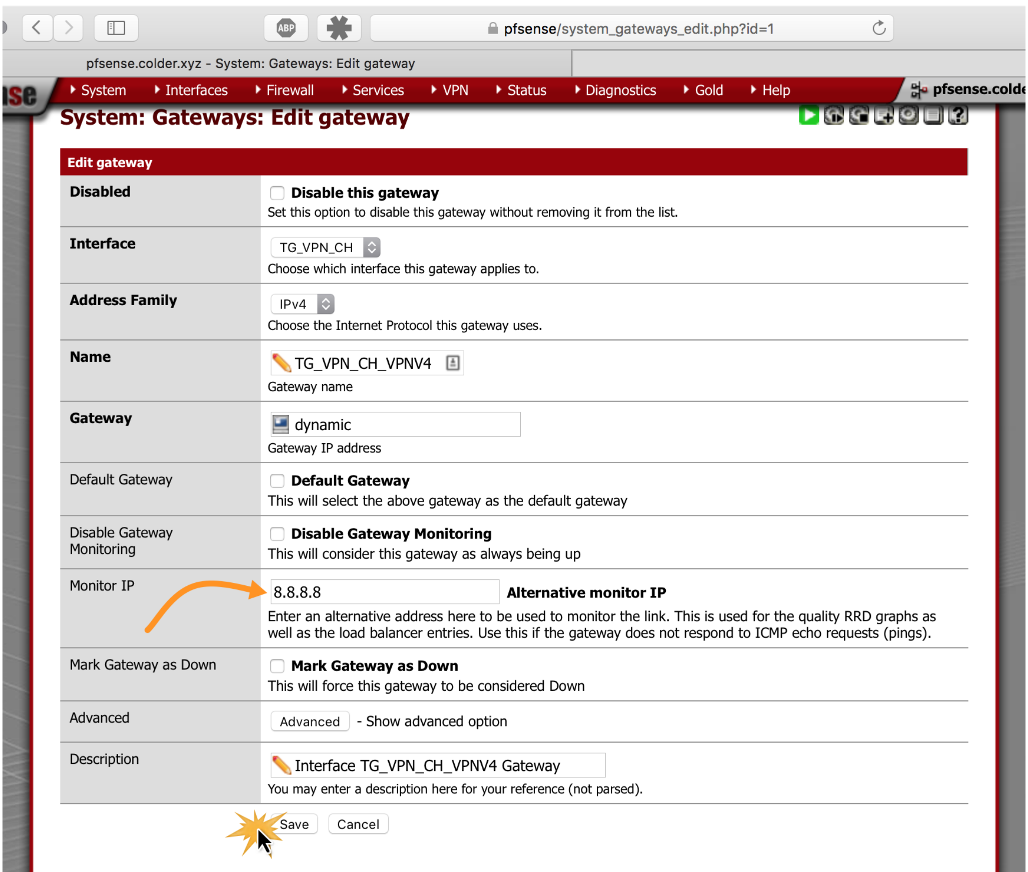


Δεν έχουμε τελειώσει με την προσθήκη του νέου κανόνα. Στην περιοχή Advanced features, λίγο πιο κάτω στη σελίδα, θέτουμε Gateway = TG_VPN_CH_VPNV4. Τα εξερχόμενα πακέτα, λοιπόν, βγαίνουν στο Internet μέσω του απομακρυσμένου TorGuard VPN server, στην Ελβετία.



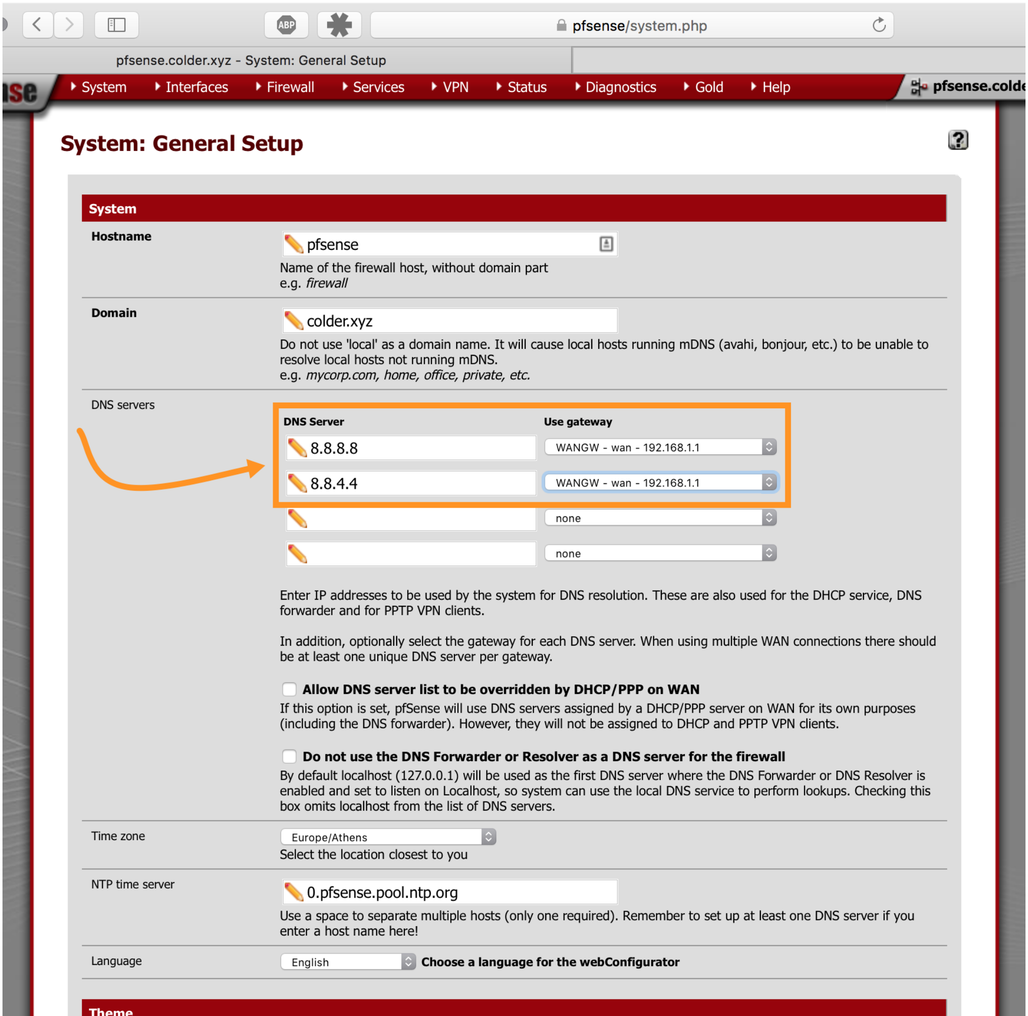
Ιδού ο ωραιότατος κανόνας μας. Για ένα πακέτο που ξεκινά από συσκευή του τοπικού δικτύου και προορίζεται για το Internet, όταν φτάνει στο OPT2 interface αρχίζουν να εξετάζονται οι κανόνες ξεκινώντας από πάνω. Εφαρμόζεται ο πρώτος που θα ταιριάξει, συνεπώς έχουμε: Αν το πακέτο προέρχεται από συσκευή της λίστας Hosts_CH, τότε εξέρχεται μέσω του TG_VPN_CH_VPNV4 (ο TorGuard VPN server). Διαφορετικά, εξέρχεται μέσω του WANGW (ο ISP μας).

Βήμα 8, ρυθμίσεις routing. Χάρη στη σύνδεση VPN που έχει επιτευχθεί, στον router μας έχει προστεθεί κι ένας νέος gateway. Στο web panel του pfSense επιλέγουμε System → Routing και στ' αριστερά της γραμμής με τον νέο gateway (ο δικός μας ονομάζεται TG_VPN_CH_VPNV4) κάνουμε κλικ στο κουμπάκι [e]. Στη νέα σελίδα που εμφανίζεται, στη θυρίδα Monitor IP βάζουμε το 8.8.8.8 και μετά πατάμε στο κουμπί Save. Ουσιαστικά, αν μέσω του κρυπτογραφημένου τούνελ προς τον server στην Ελβετία *δεν* μπορούμε να κάνουμε ping στον δημόσιο name server της Google (8.8.8.8), τότε η αντίστοιχη σύνδεση θα θεωρείται down κι ο gateway δεν θα χρησιμοποιείται.



Η κατάσταση του gateway προς τον TorGuard VPN server στην Ελβετία θα ελέγχεται με pings προς τον δημόσιο name server της Google (με IP το 8.8.8.8).

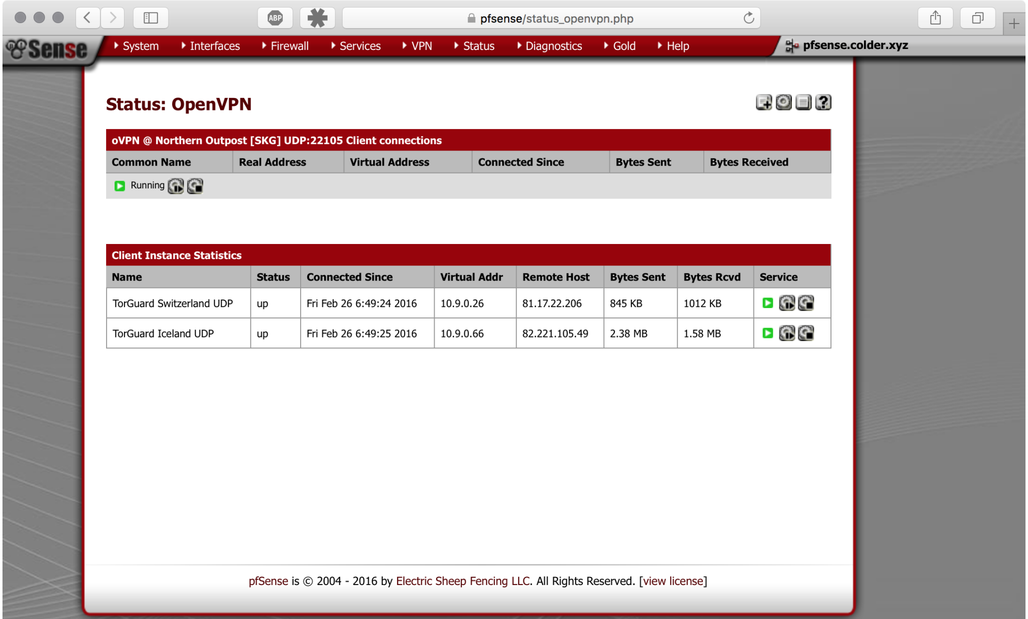
Βήμα 9, ρυθμίσεις DNS. Ολοκληρώνουμε επιτέλους την εργασία μας με μια επίσκεψη στη σελίδα System → General Setup. Στην ενότητα DNS servers, για κάθε έναν από τους δηλωμένους name servers θέτουμε το Use gateway ίσο με το WANGW - wan.



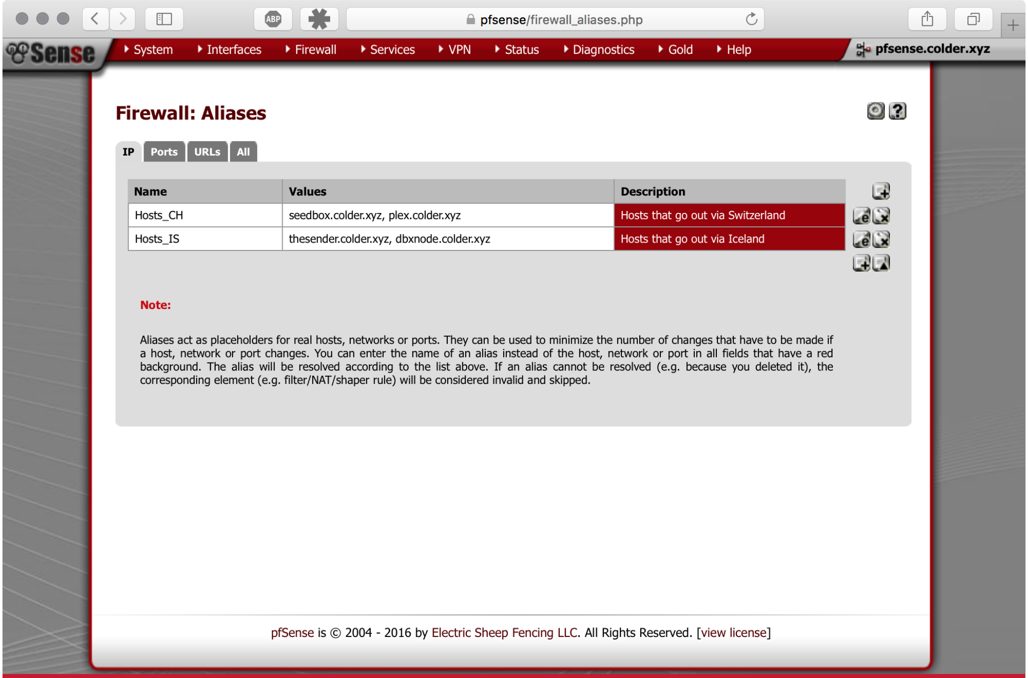
Οι δύο DNS servers που ο router μας χρησιμοποιεί είναι εκείνοι της Google (8.8.8.8 και 8.8.4.4). Τους ίδιους servers χρησιμοποιεί κι ο forwarder του συστήματος, ο οποίος εξυπηρετεί όλες τις συσκευές του τοπικού δικτύου. Φροντίζουμε ώστε σε κάθε έναν από τους δύο name servers να φτάνουμε μέσω του gateway προς τον ISP μας.

Μια σημείωση για το τέλος

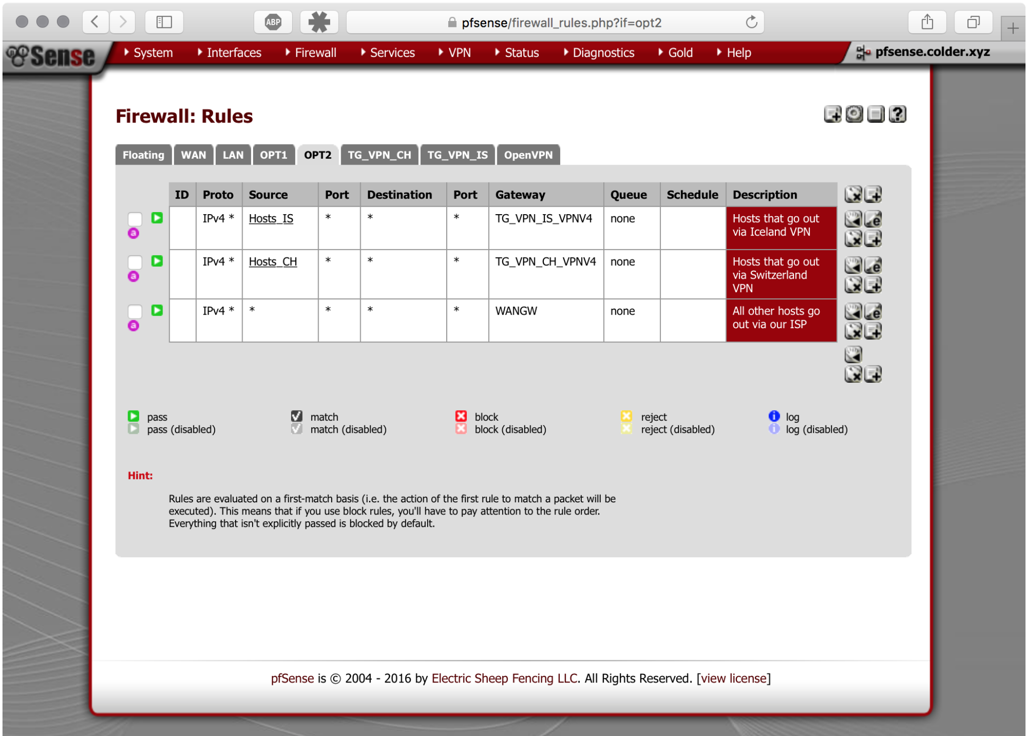
Στο σημείο αυτό διαθέτουμε ένα υποσύνολο από μηχανήματα του τοπικού μας δικτύου, τα οποία βγαίνουν έξω μέσω του TorGuard VPN server στην Ελβετία. Ξεκινώντας από το βήμα 2, κάλλιστα μπορούμε να εγκαθιδρύσουμε και μια *νέα* κρυπτογραφημένη σύνδεση προς *άλλον* TorGuard VPN server, από τον οποίο θα βγαίνουν στο Internet οι συσκευές κάποιου *άλλου* υποσυνόλου μηχανημάτων. Γενικά, για τις συσκευές που επιθυμούμε να κρύβουμε τη δικτυακή τους δραστηριότητα από τον ISP, δεν είμαστε μόνο σε θέση να ζητάμε την έξοδό τους μέσω κρυπτογραφημένου τούνελ, αλλά και να επιλέγουμε τη γεωγραφική περιοχή που βρίσκεται η έξοδος του τούνελ.



Υπάρχουν δύο OpenVPN clients ενεργοί για το pfSense box μας. Ο ένας είναι συνδεδεμένος με TorGuard server στην Ελβετία, ο άλλος με TorGuard server στην Ισλανδία.



Έχουμε δύο aliases με τοπικά hosts, τα οποία ουσιαστικά αποτελούν δύο διαφορετικά υποσύνολα δικτυωμένων συσκευών. Κάθε υποσύνολο θα βγαίνει στο Internet μέσω διαφορετικού TorGuard VPN server.



Οι κανόνες του firewall για το OPT2 interface του router μας – πρόκειται για το interface που βλέπουν οι συσκευές του τοπικού δικτύου. Όταν μία συσκευή επιχειρεί να βγει στο Internet, έχει τρεις δυνατότητες (βλ. κανόνες ξεκινώντας από πάνω): Να χρησιμοποιήσει κρυπτογραφημένο τούνελ προς TorGuard VPN server στην Ισλανδία, να χρησιμοποιήσει κρυπτογραφημένο τούνελ προς TorGuard VPN server στην Ελβετία, να μη χρησιμοποιήσει κάποιο κρυπτογραφημένο τούνελ και να βγει στο Internet απευθείας, μέσω του ISP μας.

COOKIES


.gr
Ε ΟΧΙ ΡΕ ΓΑΜΩΤΟ, ΕΛΕΟΣ!
ΤΟ EMETOS.GR ΑΝΕΒΑΣΕ ΦΩΤΟΓΡΑΦΙΕΣ ΤΟΥ ΔΙΑΜΕΛΙΣΜΕΝΟΥ ΠΤΩΜΑΤΟΣ!!!
EMETOS
ΣΟΚ: ΔΕ
ΑΥΤΟ ΕΙΝΑΙ ΚΑΝΙΒΑΛΙΣΜΟΣ, ΞΕΦΤΙΛΑ! ΘΥΣΙΑΖΟΥΝ ΤΑ ΠΑΝΤΑ ΣΤΟΝ ΒΩΜΟ ΤΟΥ ΚΛΙΚ...
ΤΣΙΦ
...ΠΣΟΦΟ ΤΟΜΑΡΙΑ...
ΜΑΡΑΚΙ, ΚΑΝΕ ΕΝΑ ΘΕΜΑ ΓΙΑ ΤΑ ΚΟΡΑΚΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ...
...ΞΕΡΕΙΣ... ΑΥΤΑ ΤΑ ΔΙΚΑ ΣΟΥ, ΤΑ ΑΡΙΣΤΕΡΑ...
ΚΑΙ ΠΟΥ 'ΣΑΙ...
...ΒΑΛΕ ΤΙΣ ΦΩΤΟΓΡΑΦΙΕΣ ΝΑ ΔΕΙ Ο ΚΟΣΜΟΣ ΓΙΑ ΤΙ ΞΕΦΤΙΛΑ ΜΙΛΑΜΕ...
ΠάΝΟΣ